Sentriant AG Software Installation Guide, Version 5.2

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: January 2009
Part number: 120501-00 Rev 01

Table of Contents

List of Figures 1

List of Tables 1

Chapter 1: What You Need to Get Started........ 1

Chapter 1: Deployment Flexibility 1

Deploying Sentriant AG Inline 4
Deploying Sentriant AG Using DHCP........4
Deploying Sentriant AG Using 802.1X........8
Installing the Network Interface Cards........11
Inline........11
DHCP........12
802.1X 12
Determining eth0 and eth1 13
Deploying Sentriant AG in VPN Mode on a Different Network........14

Chapter 1: System Requirements........ 1

General System Requirements........1
Specific System Requirements 3
Important Browser Settings........4
Pop-up Windows 4
Active Content 5
Minimum Font Size........7
Page Caching........8
Temporary Files 8
Operating Systems Supported........10
Software Supported........10
Enforcement Methods Requirements........11

Chapter 1: Installing Sentriant AG 1

Installing Sentriant AG for the First Time........1
Downloading the New Install ISO Image 1
Creating the Installation CD from the Sentriant AG Download 2
Installing Sentriant AG 3
Locating and Verifying Server Hardware........4
Information Required During Installation 5
Creating a Single-server Installation 6
Creating a Multiple-server Installation 13
Initial Configuration........14
Upgrading Sentriant AG to a Newer Version 24
Upgrading with an Internet Connection........25
Upgrading from Sentriant AG v4.x and Sentriant AG v5.0 prior to v5.0-40103........25
Upgrading from Sentriant AG v5.0-40103 or later........25

Upgrading without an Internet Connection 25
Upgrading from Sentriant AG v4.x and Sentriant AG v5.0 prior to v5.0-40103..........25
Upgrading from Sentriant AG v5.0-40103 or later..........26
Upgrading from the Command Line..........26
Upgrading from the Sentriant AG User Interface..........27
Downloading the Upgrade ISO Image 29
Creating an upgrade CD from the download..........29
Upgrading from a CD..........29

Chapter 1: Configuring Sentriant AG 1

Appendix 1: Installation and Configuration Check List 1

Minimum System Requirements..........1
Installation Location..........1
Installation Media 2
IP Addresses, Hostname, Logins, and Passwords..........2
Single-server Installation..........2
Multiple-server Installations 3
Management Server..........3
Enforcement Server 1 3
Enforcement Server 2 4
Enforcement Server 3 4
Proxy Server..........5
Agentless Credentials 5
Quarantine 6
802.1X 6
802.1X Devices 7
DHCP..........7
Accessible services..........8
Notifications..........9
Test Exceptions 10

Index.......... 1

List of Figures

Figure 1: Single-server Installation, Quarantine Method, Inline 2
Figure 2: Multiple-server Installation, Quarantine Method, Inline 2
Figure 3: Single-server Installation, Quarantine Method, DHCP, Flat Network....................3
Figure 4: Multiple-server Installation, Quarantine Method, DHCP....................3
Figure 5: Single-server Installation, DHCP Mode, Simple Example 6
Figure 6: Single-server Installation, DHCP Mode, Complex Example....................7
Figure 7: Single-server Installation, Endpoint Static Route Enforcement....................8
Figure 8: 802.1X Enforcement 10
Figure 9: Single-server Installation, Ethernet Card Installation, Inline....................11
Figure 10: Single-server Installation, Ethernet Card Installation, DHCP 12
Figure 11: Single-server Installation, Ethernet Card Installation, 802.1X....................13
Figure 1: Internet Explorer Security Warning Message....................5
Figure 2: IE Security Message Options 6
Figure 3: IE Security Warning Pop-up Window....................6
Figure 4: IE Internet Options, Advanced Tab....................6
Figure 1: Install Screen, Boot Prompt....................7
Figure 2: Install Screen, Installation Confirmation 8
Figure 3: Install Screen, Network Configuration for eth0 9
Figure 4: Install Screen, Miscellaneous Network Settings....................9
Figure 5: Install Screen, Hostname Configuration....................10
Figure 6: Install Screen, Time Zone Selection 11
Figure 7: Install Screen, Root Password....................12
Figure 8: Install Screen, Installation Type....................12
Figure 9: Install Screen, Installation Progress 13
Figure 10: Security Alert Window....................15
Figure 11: Accept License Agreement Window 16
Figure 12: Enter Management Server Settings Window....................17
Figure 13: Enter License Key Window 18
Figure 14: Create Administrator Account Window 19
Figure 15: Sentriant AG Home Window 20
Figure 16: Enforcement Clusters & Servers....................21
Figure 17: Add Enforcement Cluster Window 22
Figure 18: Add Enforcement Server Window 23
Figure 19: System Configuration, Enforcement Clusters & Servers Window 24
Figure 20: System Configuration Window, Management Server Option....................28

List of Tables

Table 1: Sentriant AG System Requirements 1

1 What You Need to Get Started

You need the following prior to installing and running Sentriant AG:

- **Minimum system (hardware and software) requirements**—See "System Requirements" on page 1
- **IP addresses you will enter during the set up process**—See "Installation and Configuration Check List" on page 1
- **Install CD**—See "Installing Sentriant AG" on page 3

This Installation Guide helps you install and set up Sentriant AG. The *Sentriant AG Users Guide* (available on the CD in the `/docs` directory and through the online help links in Sentriant AG) provides Sentriant AG configuration information and task-based instructions.

1 Deployment Flexibility

Sentriant AG Version 5.2 allows you to deploy multiple Enforcement servers (ESs) across a network and manage them from one central Management server (MS). You create logical groups of ESs by joining them to an Enforcement cluster.

The Sentriant AG MS specifies many aspects of the Enforcement clusters; for example, the MS specifies the enforcement method (inline, DHCP, or 802.1X), how often the endpoints are retested, the tests run on the endpoints, and how to control the endpoints' access.

The Sentriant AG ESs detect and test endpoints on the network for compliance.

You can deploy each Sentriant AG cluster in one of the following configurations:

- **Inline—**When deploying Sentriant AG inline, Sentriant AG monitors and enforces all endpoint traffic. When Sentriant AG is deployed as a single-server installation, Sentriant AG becomes a Layer 2 bridge that requires no changes to the network configuration settings. When Sentriant AG is installed in a multiple-server installation, you might have to configure the switch that connects the Sentriant AG Enforcement servers to use Spanning Tree Protocol (STP) if STP is not already configured. Sentriant AG allows endpoints to access the network or blocks endpoints from accessing the network based on their Internet Protocol (IP) address with a built-in firewall (iptables).
- **DHCP—**When deploying Sentriant AG inline with a *Dynamic Host Configuration Protocol* (DHCP) server, all DHCP requests pass through the Sentriant AG server Layer 2 bridge. For a quarantined endpoint, Sentriant AG distributes the quarantined IP address for the endpoint. If Sentriant AG allows the endpoint to have access, Sentriant AG allows your real DHCP server to distribute a non-quarantined IP address. Sentriant AG assigns a DHCP IP address based on the quarantine area parameters you define during configuration. You can place restrictions on network access either at the gateway for the endpoint using Access Control Lists (ACLs), or on the endpoint by removing the endpoint's gateway and adding static routes for accessible networks.
- **802.1X—**When deploying Sentriant AG in an 802.1X environment, you must install it where it can communicate with the Remote Authentication Dial-In User Service (RADIUS) server (or, Sentriant AG has a built-in RADIUS server that you can use). The RADIUS server communicates with the switch, which performs the quarantining by moving ports or MAC addresses in and out of virtual local area networks (VLANs).

The following figures illustrate various deployment methods.

Figure 1: Single-server Installation, Quarantine Method, Inline

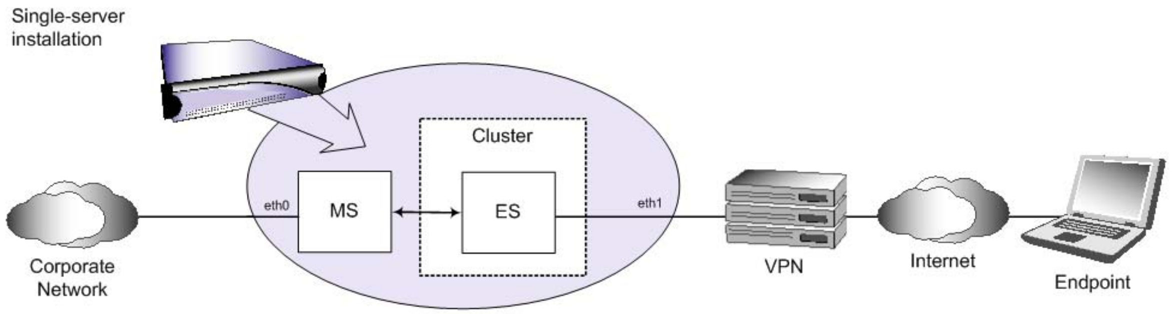


Figure 2: Multiple-server Installation, Quarantine Method, Inline

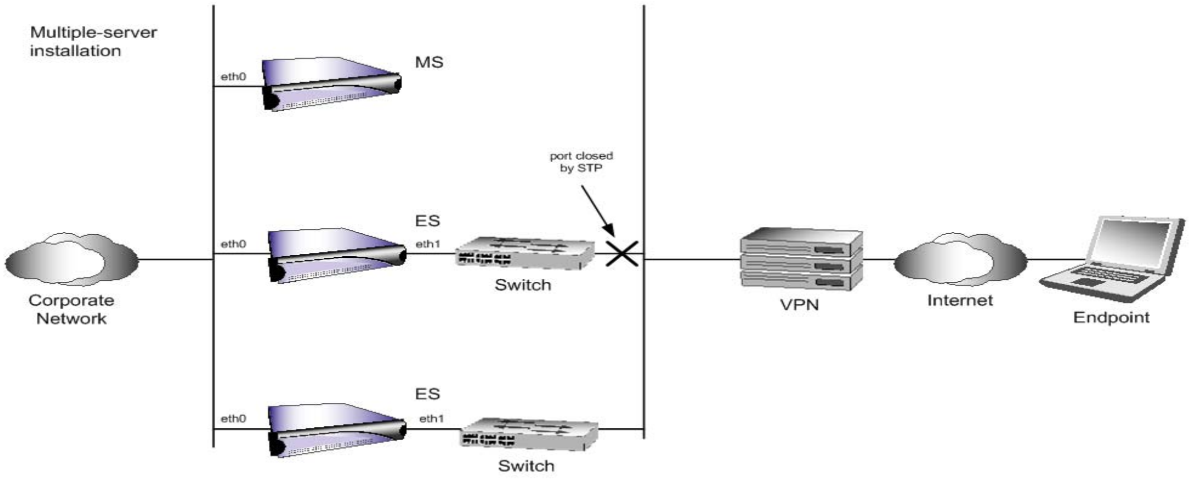


Figure 3: Single-server Installation, Quarantine Method, DHCP, Flat Network

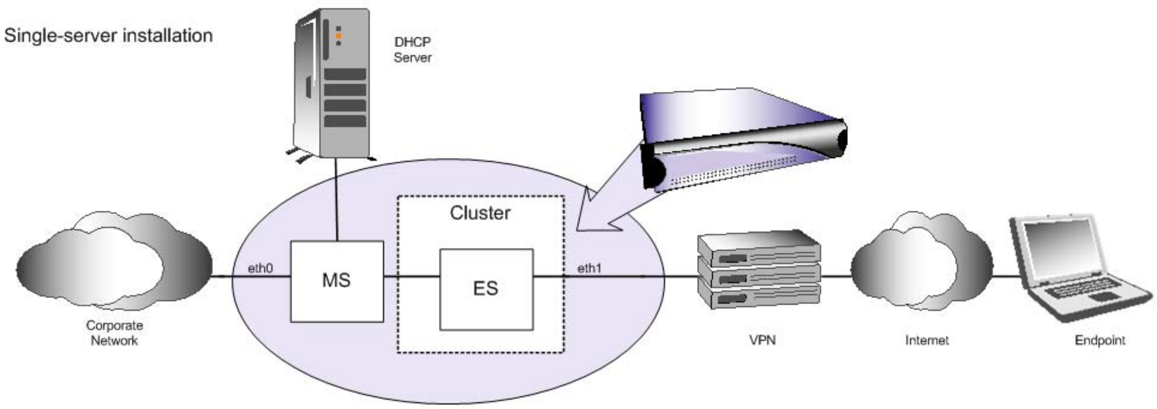
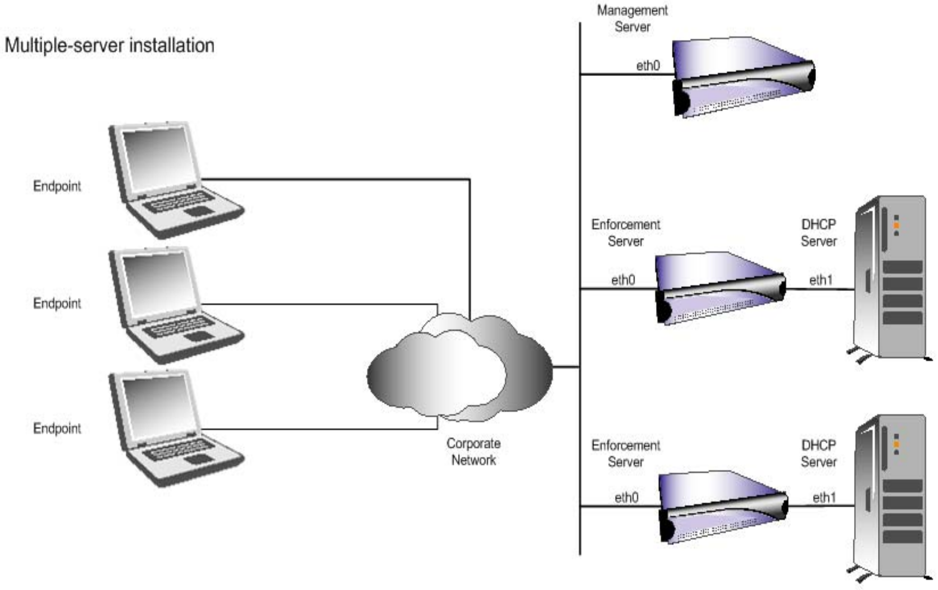


Figure 4: Multiple-server Installation, Quarantine Method, DHCP



Deploying Sentriant AG Inline

The ES's position in the network is between the endpoints and the rest of the network; acting as a gateway and only allowing endpoints access to network resources that have met the necessary security requirements. Sentriant AG uses two network interfaces to bridge traffic between endpoints and the rest of the network. Sentriant AG uses a high-speed, Layer 2 bridge; network IP address changes are not required. Since Sentriant AG *itself* denies endpoints access to the network, policy enforcement using internal routers, switches, or other endpoints is not required.

Sentriant AG utilizes a pass-through authentication feature that allows it to work with any virtual private network (VPN), remote access server (RAS), and network authentication protocol or directory.

By default, an onboard firewall blocks all traffic from endpoints. Sentriant AG allows network access to only successfully tested endpoints (or when there is a grace period for failed tests). When a test or tests pass, Sentriant AG inserts rules into the onboard firewall to allow all traffic from the endpoint. Sentriant AG uses a proprietary method to uniquely identify each endpoint as it connects to the network, and does not install cookies or software on the end-user's endpoint.

NOTE

When the MS and ES are installed on the same server (single-server Installation), that server's position in the network must be between the endpoints and the rest of the network.

Deploying Sentriant AG Using DHCP

When you configure Sentriant AG with a DHCP quarantine area, the Sentriant AG ES must sit inline with your DHCP server. If this is not possible, you must configure a remote host for Device Activity Capture (DAC) as described in the User's Guide, Remote Device Activity Capture with a quarantined endpoint, the ES responds to the DHCP request and blocks the request from getting to the main DHCP server. When the endpoint is allowed access, Sentriant AG does not respond to the DHCP request and lets the request through to the main DHCP server which responds with normal DHCP settings. The Sentriant AG DHCP server can respond to quarantined endpoints with one of these two types of DHCP settings:

- **DHCP settings for a separate quarantine subnetwork**—In this case, network access is restricted by adding ACLs to your router between the quarantine subnetwork and all other networks. You must also add an IP helper address for the Sentriant AG ES, and a secondary IP address for the quarantined subnetworks gateway to the router.
- **DHCP settings using static routes**—In this case, network access is restricted by giving the endpoint a normal IP address but not assigning a gateway. The advantage of this method is that it requires only one router change to add an IP helper address for the Sentriant AG ES. Also, some routers do not like multi-netting, which is required by the first method and not by this method of DHCP enforcement. The Sentriant AG ES uses the following DHCP settings:
  - **Gateway**—None
  - **Netmask**—255.255.255.255
  - **DNS**—Sentriant AG ES IP address
  - **Static routes**—Configurable list of accessible IP addresses and networks

These DHCP settings effectively restrict all network access except to the IP addresses and networks specified as static routes in the accessible endpoints and services area. A list of Web sites can also be configured as accessible. You can access these Web sites through a proxy server, which is built into the Sentriant AG ES. The Sentriant AG ES responds to DHCP INFO requests to automatically configure the proxy server in the browser.

Once the endpoint is allowed access, the IP address is automatically renewed and the main DHCP server assigns an IP address in the main LAN.

NOTE

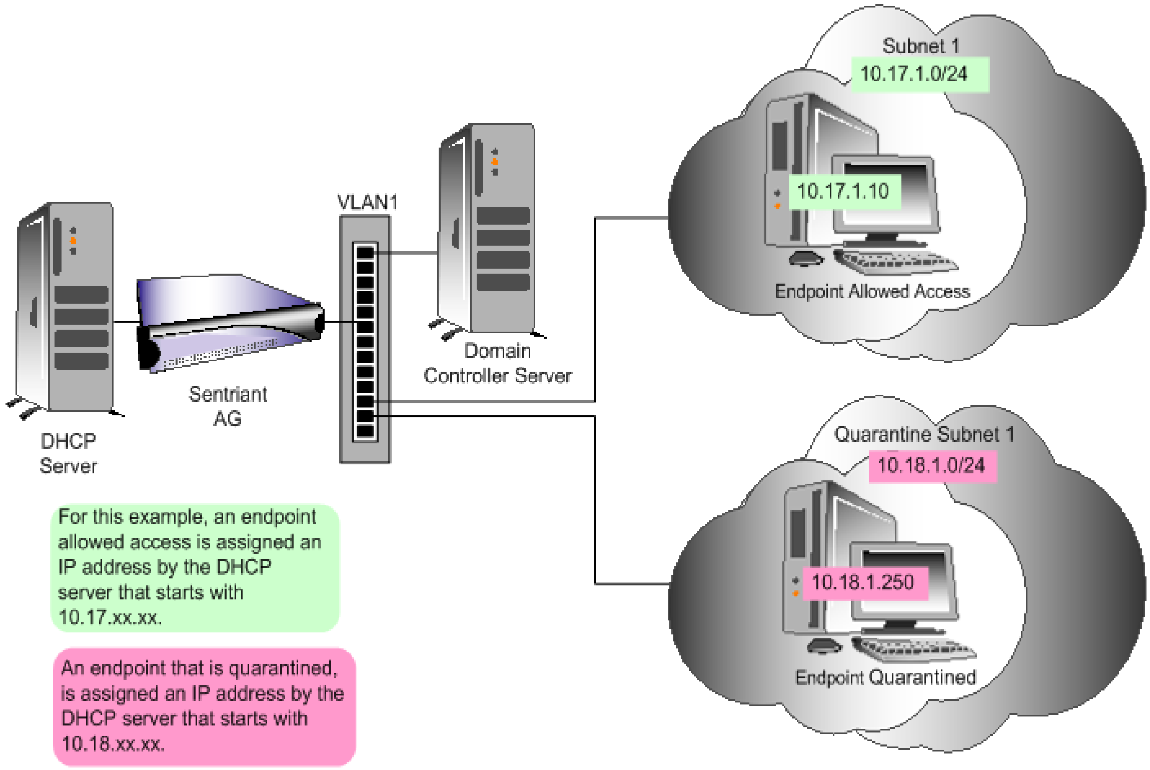
When the MS and ES are installed on the same server (single-server Installation), that server’s position in the network must be inline with your DHCP server. It is the ES that responds to the DHCP request and blocks the request from getting to the main DHCP server.

NOTE

When using DHCP mode and connecting directly to the DHCP server's network interface, be sure to use a crossover cable.

The following figure shows an example installation scenario for a simple (one LAN) setup with enforcement using ACLs on a router.

Figure 5: Single-server Installation, DHCP Mode, Simple Example

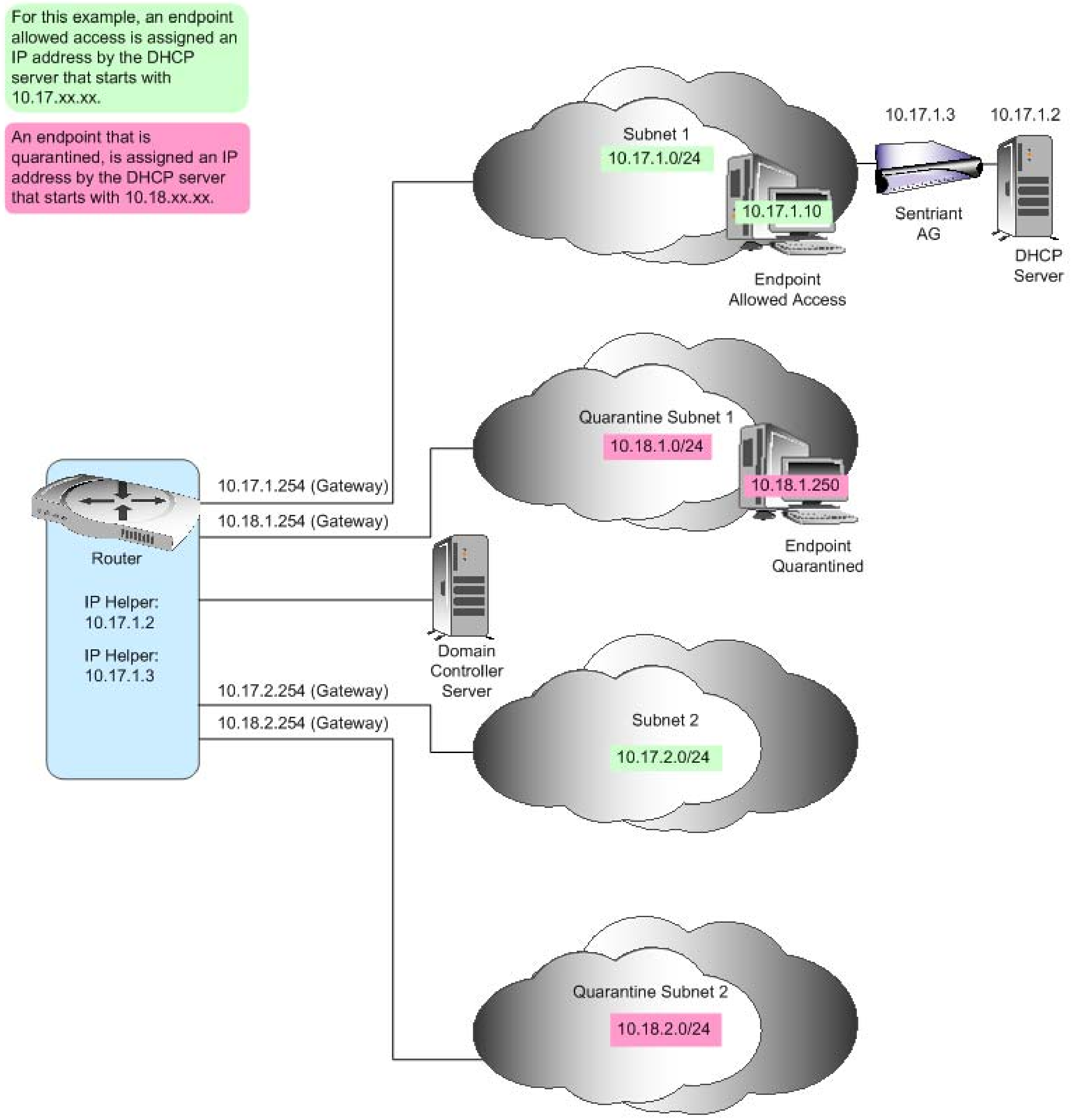


For this example, an endpoint allowed access is assigned an IP address by the DHCP server that starts with 10.17.xx.xx.

An endpoint that is quarantined, is assigned an IP address by the DHCP server that starts with 10.18.xx.xx.

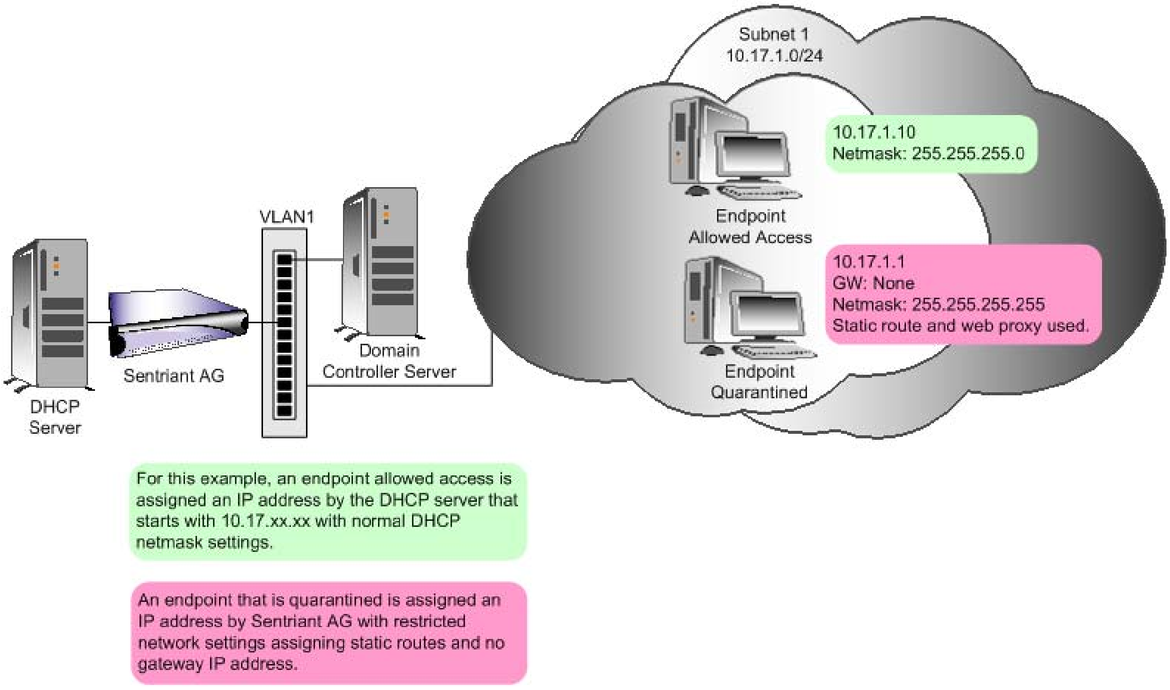
The following figure shows an example installation scenario for a complex (multiple LAN) setup with enforcement using ACLs on a router.

Figure 6: Single-server Installation, DHCP Mode, Complex Example



The following figure shows an example installation scenario for a setup with enforcement with static routes on the endpoint.

Figure 7: Single-server Installation, Endpoint Static Route Enforcement



10.17.1.10
Netmask: 255.255.255.0

10.17.1.1
GW: None
Netmask: 255.255.255.255
Static route and web proxy used.

For this example, an endpoint allowed access is assigned an IP address by the DHCP server that starts with 10.17.xx.xx with normal DHCP netmask settings.

An endpoint that is quarantined is assigned an IP address by Sentriant AG with restricted network settings assigning static routes and no gateway IP address.

Deploying Sentriant AG Using 802.1X

To configure Sentriant AG as 802.1X-enabled, install it with one of three different configurations, depending on your network environment (see Figure 8):

1 Use the built-in Sentriant AG RADIUS server to proxy to any other RADIUS server. In this configuration, the switch performs the 802.1X authentication against the Sentriant AG RADIUS server, which proxies the request to another RADIUS server. During the return proxy of the authentication request, the Sentriant AG ES instructs the switch in which VLAN is to place the endpoint based on its test status.

2 Use the built-in Sentriant AG RADIUS server and user accounts. In this configuration, the switch performs the 802.1X authentication against the Sentriant AG RADIUS server. The Sentriant AG ES instructs the switch in which VLAN to place the endpoint, based on its test status.

3 Use the IAS plug-in to integrate with your existing radius server. In this configuration, the switch performs the 802.1X authentication against the Microsoft Internet Authentication Service (IAS) RADIUS server. A Sentriant AG plug-in to the IAS RADIUS server is available that instructs the switch in which VLAN to place the endpoint based on its test status.

NOTE

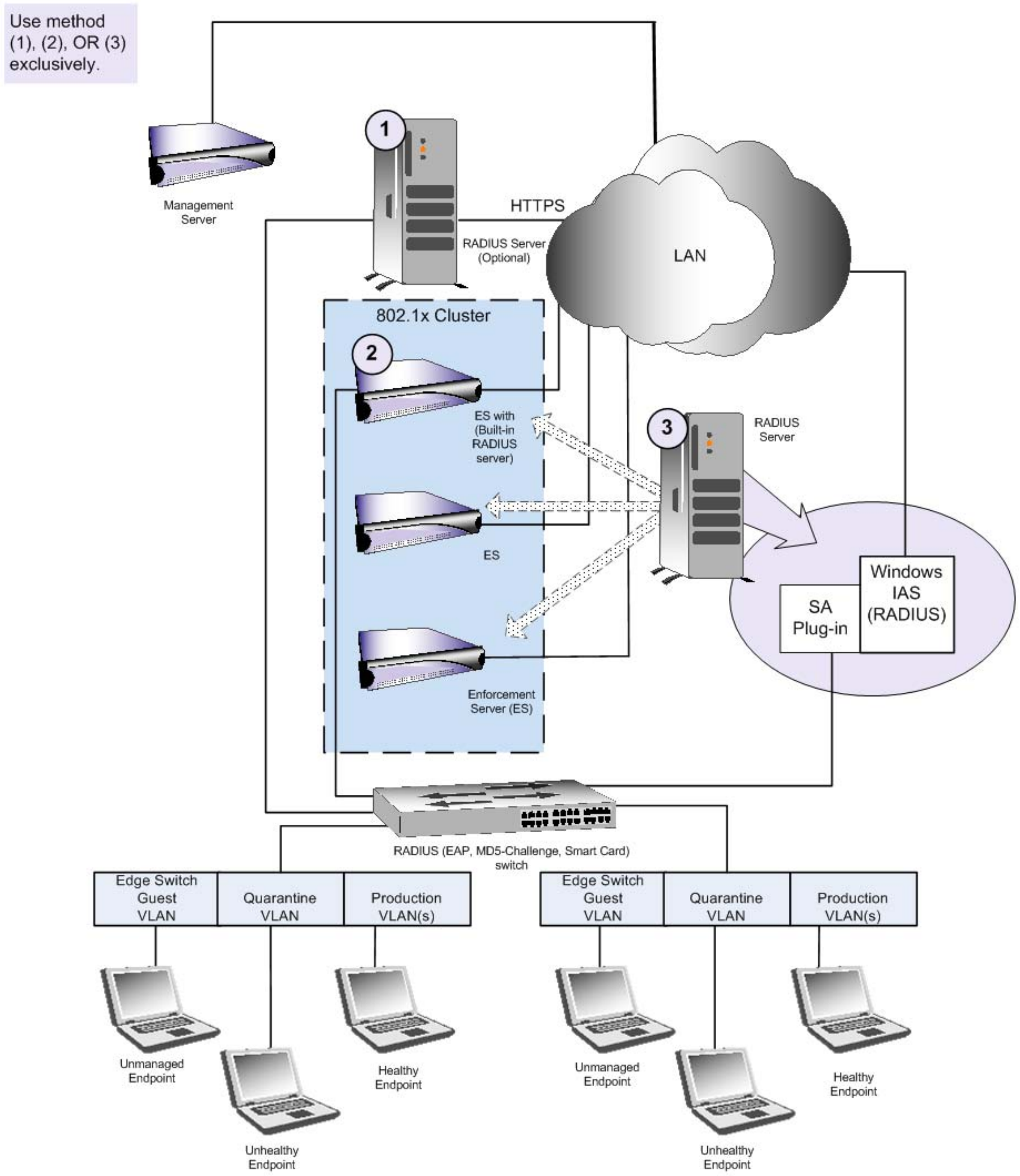
With a single-server Installation, the ES instructs the switch in which VLAN to place the endpoint.

NOTE

If the ES cannot see traffic on a mirrored port on a switch, you must configure a remote host for Device Activity Capture (DAC) as described in the User's Guide, Remote Device Activity Capture.

A sample deployment is shown in the following figure:

Figure 8: 802.1X Enforcement



Installing the Network Interface Cards

The number of network interface cards (NICs) required depends on the installation method selected as described in this section.

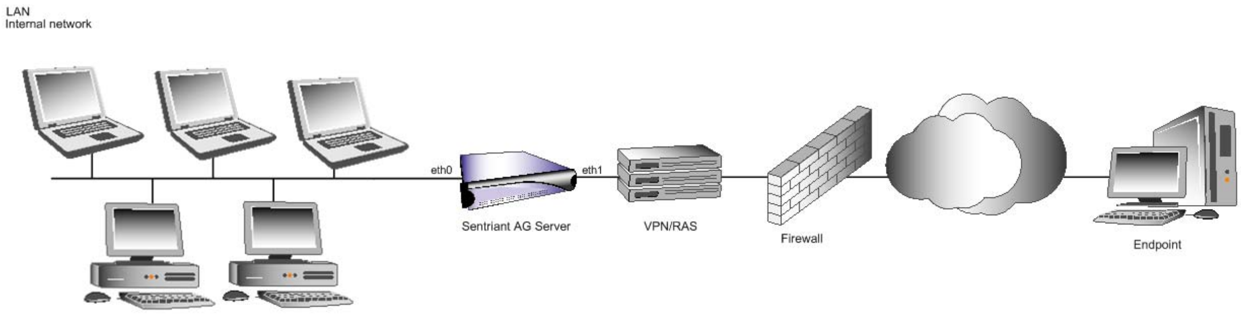
Inline

The inline installation of Sentriant AG, where the MS and ES are installed on a single server, requires two network interface cards (NICs) installed for Sentriant AG to operate properly.

The inline installation of Sentriant AG where the MS and ES are installed on different servers requires at least three NICs; one for the MS and two for each ES.

The inline installation interfaces form a bridge from one part of your network to another as shown in the following figure. The Linux® operating system assigns each interface a name (for example, `eth0`, `eth1`, and so on). It is very important that you connect the `eth0` interface to your local area network (LAN) side, and `eth1` to the Virtual Private Network (VPN) side (for inline mode or for the main DHCP server in DHCP mode).

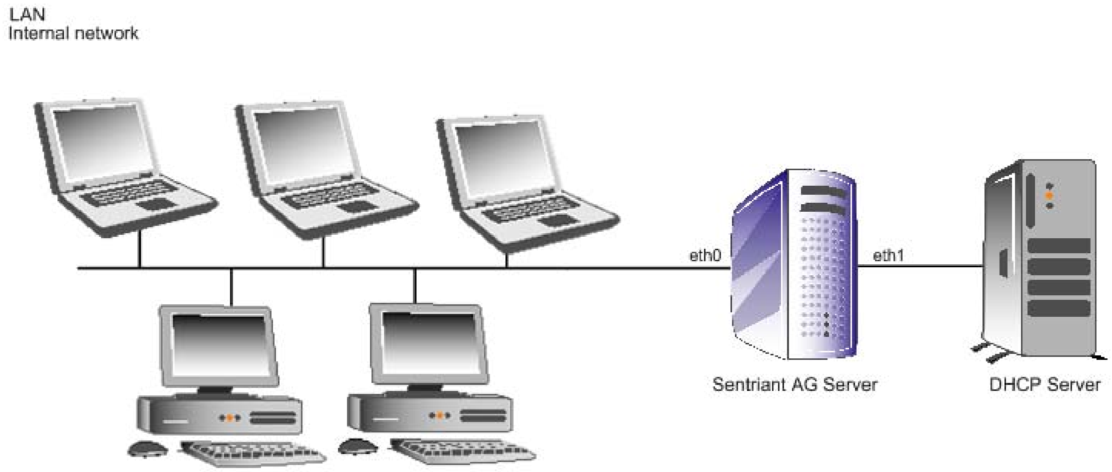
Figure 9: Single-server Installation, Ethernet Card Installation, Inline



DHCP

A DHCP installation requires two NICs where the MS and ES are installed on the same server (see Figure 10), and at least three NICs where the MS and ES are installed on different servers; one for the MS and two for each ES.

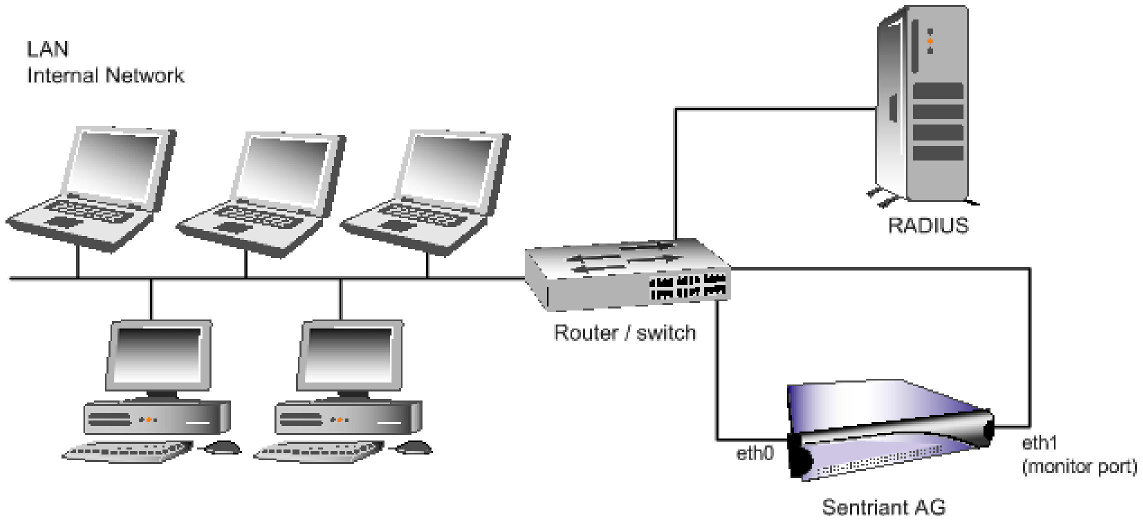
Figure 10: Single-server Installation, Ethernet Card Installation, DHCP



802.1X

802.1X-enabled Sentriant AG installations require one NIC where the MS and ES are installed on the same server (see Figure 11), and two NICs where the MS and ES are installed on different servers. In 802.1X mode, `eth1` on Sentriant AG is used to discover endpoints on the network. To discover endpoints on the local network, `eth1` can simply be plugged into a port on that subnet because it receives broadcast traffic. To discover endpoints on other networks, `eth1` must be connected to a mirrored port or a port that is part of a tagged VLAN trunk to detect traffic from endpoints on these other networks. Usually, mirroring the ports in which the DNS and DHCP server resides detects new endpoints sufficiently.

Figure 11: Single-server Installation, Ethernet Card Installation, 802.1X



NOTE

It is strongly recommended that you use the Intel NIC cards. If you use a different NIC card, you might be unable to connect, or experience unpredictable results and availability.

Determining eth0 and eth1

To determine which interface is eth0 and which is eth1 using ethtool:

1 After installing Sentriant AG, plug an Ethernet cable into only one of the interfaces.

2 Log into the Sentriant AG MS as `root` and enter one of the following commands:

   a `et`htool eth0

   b `ethtool -p eth`*`n`* `x`

   Where:
   n is the number of the Ethernet interface, for example 0
   x is the number of seconds to allow the lights to blink

3 The return values are similar to the following, which also indicates that the connected interface is `eth0`:

```
# ethtool eth0
Settings for eth0:
     Supported ports: [ MII ]
     Supported link modes:     10baseT/Half 10baseT/Full
                               100baseT/Half 100baseT/Full
                               1000baseT/Half 1000baseT/Full
     Supports auto-negotiation: Yes
     Advertised link modes:    10baseT/Half 10baseT/Full
                               100baseT/Half 100baseT/Full
                               1000baseT/Half 1000baseT/Full
     Advertised auto-negotiation: Yes
     Speed: 100Mb/s
     Duplex: Full
     Port: Twisted Pair
     PHYAD: 1
     Transceiver: internal
     Auto-negotiation: on
     Supports Wake-on: g
     Wake-on: d
     Current message level: 0x000000ff (255)
     Link detected: yes
```

NOTE

In normal operation, Sentriant AG does not respond to Internet Control Message Protocol (ICMP or ping) echo requests.

Deploying Sentriant AG in VPN Mode on a Different Network

When Sentriant AG is deployed in VPN mode, the eth1 interface on Sentriant AG is usually connected directly (either by way of a crossover cable, isolated switch, or VLAN) to the LAN-facing side of the VPN concentrator. If the same logical subnet (such as, 10.10.0.0/16) is used for Sentriant AG, the concentrator, and the VPN clients, no modifications need be made.

However, problems can arise if the following conditions are all true:

- Sentriant AG is in a different logical subnet than that used by the VPN concentrator OR the VPN client endpoints.
- The router on the LAN (eth0) side of Sentriant AG is configured for best-practices egress filtering, and will not route packets that have a source IP address outside the network segment from which they appear to originate.

  See the SANS Egress Filtering FAQ, http://www.sans.org/reading_room/whitepapers/firewalls/1059.php for a more thorough discussion of egress filtering.

The most obvious symptom of this situation is that Sentriant AG will not be able to redirect endpoint clients (they will get a blank browser page that appears to take forever to load) but the endpoint browser is able to browse directly to `https://`*<Sentriant AG_IP_Address>*`:89/` and get tested.

For example, for the following IP addresses:

- **Router IP—**10.1.90.254, on a /24
- **Sentriant AG IP—**10.1.90.130, on a /24
- **VPN concentrator IP—**10.1.90.131, on a /24
- **VPN client IP range—**10.1.105.0/24

The VPN concentrator is configured to hand out IP addresses on the 10.1.105.0/24 subnet, while Sentriant AG and the VPN concentrator itself are on the 10.1.90.0/24 subnet. Both Sentriant AG and the VPN concentrator have a default route set through 10.1.90.254 which is a router or Layer 3 switch on the LAN (eth0) side of Sentriant AG.

Because a connecting VPN endpoint is not on the same subnet as Sentriant AG, all of the packets that Sentriant AG sends (in response to HTTP requests from the endpoint) go to the router at 10.1.90.254, which knows to send them (back through the Sentriant AG bridge) to the VPN concentrator for a next hop. For normal communication (such as testing traffic) between Sentriant AG and an endpoint, this works fine, even if it seems a bit inefficient.

However, when Sentriant AG redirects an HTTP connection, it first constructs an HTTP redirect with a source IP address corresponding to the original destination of the connection.

For example:

1 The endpoint connects to the VPN, and the browser requests www.google.com.

2 Sentriant AG intercepts the packets addressed to google.com.

3 Sentriant AG constructs an HTTP redirection to the Sentriant AG IP, using packets which have a source IP address of www.google.com.

4 Sentriant AG sends the constructed redirect to the VPN endpoint using the Sentriant AG default route.

Those packets go to the LAN side router, which in our scenario is configured with best-practices egress filtering. The router treats those packets as errors (because they are marked with a source IP address that should not emanate from that network segment) and drops them. This is why testing works when the endpoint connects directly to emanate—the response packets still go to the LAN-side router, but it routes them appropriately because they have a valid source address.

The solution is to add a static route to Sentriant AG so that it knows to send packets addressed to 10.1.105 via the VPN concentrator instead of the LAN-side router, and it will redirect correctly.

You also want to make the static route addition permanent across reboots.

To add a permanent static route to the Sentriant AG server:

1 Log in as root to the Sentriant AG server using SSH or directly with a keyboard.

2 Open the following file with a text editor, such as vi.

```
/etc/rc.local
```

3 Add something like the following:

```
#
```

```
# explicit routes for VPN subnets should go to the VPN router,
# not the default gateway
#
/sbin/route add -net 10.1.105.0/24 gw 10.1.90.131
```

Where, for other network configurations or additional VPN profiles you need to add routes appropriate to the subnet or subnets involved.

1 System Requirements

There are several required elements you must have or configure when setting up your network for Sentriant AG:

- "General System Requirements" on page 1
- "Specific System Requirements" on page 3
- "Enforcement Methods Requirements" on page 11

General System Requirements

The following hardware and software is required to install and operate Sentriant AG.

Table 1: Sentriant AG System Requirements

Item	Required
Server—A dedicated server or servers for product installation with the following minimum system requirements:	

Table 1: Sentriant AG System Requirements

Item		Required
	Processor	Intel Dual Core (Core 2 Duo/Xeon 5100 series) processor at 1.86 GHz (or greater)
	RAM	2 GB RAM (or greater)
	Disk space	80 GB SATA disk (or greater)
	Multiple-server installation: **MS installation**—One server-class network interface cards (NICs) and— **ES installation**— **DHCP**—Two server-class network interface cards (NICs) **Inline**—Two server-class network interface cards (NICs) **802.1x-enabled installation**—One server-class network interface cards **Single-server installation**—Two server-class network interface cards (NICs)	10/100/1000 (Intel)
	CD-ROM drive	yes
	An Internet connection or a web proxy server that allows outbound HTTPS communications from the MS.	yes
Workstation—A workstation running one of the following browsers: • **Windows**— Mozilla version 1.7 Mozilla Firefox version 1.5 or later Internet Explorer 6.0 • **Linux**— Mozilla version 1.7 Mozilla Firefox version 1.5 or later • **Mac OS X**— Mozilla Firefox version 1.5 or later		yes
License—A license key		yes
Product updates—The latest Sentriant AG product updates		yes

NOTE

The hardware and memory requirements for Sentriant AG v5.0 are not the same as older versions. The software will not prevent you from upgrading; however, you may experience performance issues if your hardware and memory are less than that specified.

NOTE

It is strongly recommended that you use the server-class Intel NIC cards. If you use a different NIC card, you might be unable to connect, or experience unpredictable results and availability.

NOTE

Your license key is emailed to you. If you did not receive one, contact Extreme Networks, Inc. Technical Assistance Center (TAC) (support@extremenetworks.com or (800) 998-2408).

Specific System Requirements

The following hardware is supported for this version of Sentriant AG, although other hardware may also function properly:

- Server (hosting Sentriant AG):
  The following servers are supported only when used with hardware listed in the *Sentriant AG Installation guide* and the *Sentriant AG Users' guide*.
  - Dell 1950 Multi-core Intel, 2 GB or higher RAM, with SATA or SAS drives
  - Dell 2950 Multi-core Intel, 2 GB or higher RAM, with SATA or SAS drives
  - HP ProLiant DL360 G5 with SAS drives
  - IBM System x3550 with SAS drives
- NIC card:
  - Intel Pro 100/1000
- HA Bypass Card
  - Niagara 2261 bypass card (PCI-X)
  - Niagara 2265 bypass card (PCIe)
- VPN:
  - Cisco VPN Concentrators
  - OpenSSL VPNs
- Switches:
  - Cisco
    4005 CATOS (software version 8.4 (9) GLX)
    6509 CATOS (software version 8.5 (7))
    2950 IOS (software version 12.1 (22) EA8a)
    3750 IOS ipbase 12.2(25) SEB

- Enterasys
  1H582-25 (software version 03.05.06)
- Extreme
  Extreme Network Switches running EXOS version 11.2.2.4 or later
- Foundry
  FastIron Edge 9604 (software version FES 3.5 and above)
  FastIron Edge (FES) 4802 (software version FES 3.4 and above)
- HP
  - ProCurve 3400cl-24G (software version M.10.20)
  - ProCurve 2650 (software version H.08.86)
  - ProCurve 2824 (software version I.08.105)
  - ProCurve 2900 (software version T.11.X1)
  - ProCurve 3500yl (software version K.12.01)
  - ProCurve 5340xl (software version E.10.52)
- Nortel
  - BayStack 5510—v4.2.0.002
  - BayStack 5510—5530_423024.img (for 5510, 20, 30)
  - BayStack 5510—5530_423025s.img (for 5510, 20, 30)
  - BayStack 5510—5530_503004.img (for 5510, 20, 30)
  - BayStack 5510—5530_503005s.img (for 5510, 20, 30)

NOTE

VMware is not supported.

Important Browser Settings

Pop-up Windows

The Sentriant AG reports capability uses a pop-up window. In order for you to run reports on Sentriant AG, you *must* allow pop-up windows from the Sentriant AG server.

To allow pop-up windows in Internet Explorer:

Internet Explorer browser>>Tools>>Pop-up blocker>>Pop-up blocker settings

1 Enter the IP address or partial IP address of the Sentriant AG MS.

2 Click **Add**.

3 Click **Close**.

To allow pop-up windows in Mozilla:

Mozilla browser>>Edit>>Preferences>>Privacy & Security>>Popup Windows

1. Select the **Block unrequested popup windows** check box.
2. Click **Allowed sites**.
3. Enter the IP address or partial IP address of the Sentriant AG MS.
4. Click **Add**.
5. Click **OK**.
6. Click **OK**.

To allow pop-up windows in Windows or Linux Firefox:

Firefox browser>>Tools>>Options>>Content

1. Clear the **Block Popup Windows** check box.
2. Click **OK**.

To allow pop-up windows in Mac Firefox:

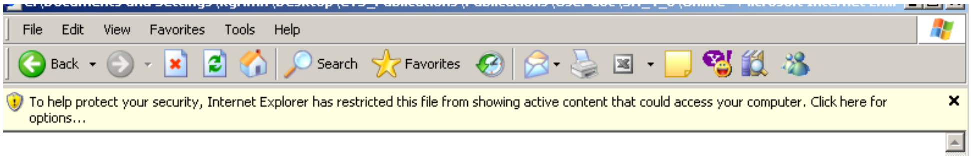
Firefox menu>>Preferences>>Content

1. Clear the **Block Popup Windows** check box.
2. Close the **Content** window.

Active Content

If you see the following Active Content message at the top of the browser window when you access the Sentriant AG help feature. perform the instructions in this section to allow Active Content to display.

Figure 1: Internet Explorer Security Warning Message

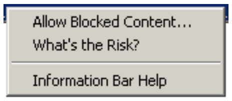


To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...

To allow Active Content to display:

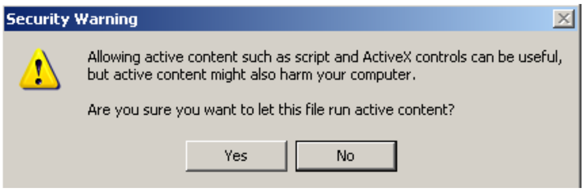
1 Click on the message box to display the options (Figure 2).

Figure 2: IE Security Message Options



2 Select **Allow Blocked Content**. The **Security Warning** window appears:

Figure 3: IE Security Warning Pop-up Window



Allowing active content such as script and ActiveX controls can be useful, but active content might also harm your computer.

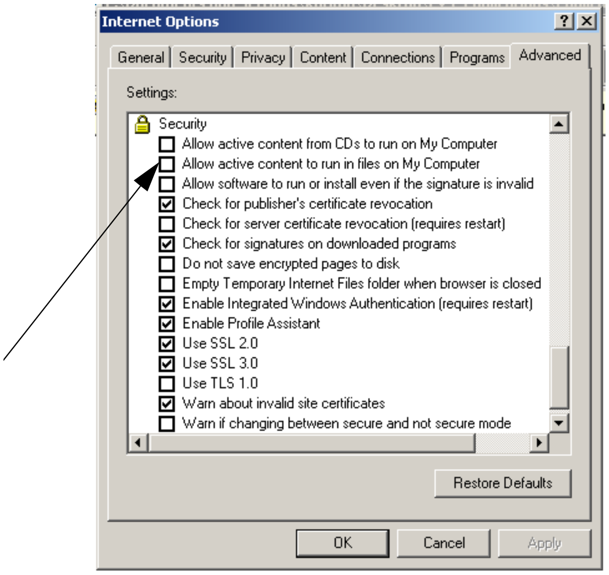
Are you sure you want to let this file run active content?

3 Click **Yes** on the **Security Warning** window.

To change the Internet Explorer security settings to always allow active content:

IE browser>>Tools>>Internet Options>>Advanced tab

Figure 4: IE Internet Options, Advanced Tab



Settings:

Security
- □ Allow active content from CDs to run on My Computer
- □ Allow active content to run in files on My Computer
- □ Allow software to run or install even if the signature is invalid
- ☑ Check for publisher's certificate revocation
- □ Check for server certificate revocation (requires restart)
- ☑ Check for signatures on downloaded programs
- □ Do not save encrypted pages to disk
- □ Empty Temporary Internet Files folder when browser is closed
- ☑ Enable Integrated Windows Authentication (requires restart)
- ☑ Enable Profile Assistant
- ☑ Use SSL 2.0
- ☑ Use SSL 3.0
- □ Use TLS 1.0
- ☑ Warn about invalid site certificates
- □ Warn if changing between secure and not secure mode

1 In the **Internet Options** pop-up window, scroll down to the security section.

2 Select the **Allow active content to run in files on my computer** check box.

3 Click **OK**.

Minimum Font Size

In order to properly display the Sentriant AG user interface, do not specify the minimum font size.

To clear the Internet Explorer minimum font size:

IE browser>>Tools>>Internet options>>General tab>>Accessibility button

1 Make sure all of the check boxes are cleared on this window.

2 Click **OK**.

3 Click **OK**.

To clear the Mozilla minimum font size:

Mozilla browser>>Edit>>Preferences>>Appearance>>Fonts

1 Select **None** from the **Minimum font size** drop-down list.

2 Click **OK**.

To clear the Windows or Linux Firefox minimum font size:

Firefox browser>>Tools>>Options>>Content>>Fonts & Colors, Advanced

1 Select **None** in the **Minimum font size** drop-down list.

2 Select the **Allow pages to choose their own fonts, instead of my selections above** check box.

3 Click **OK**.

4 Click **OK**.

To clear the Mac Firefox minimum font size:

Firefox menu>>Preferences>>Content>>Fonts & Colors, Advanced

1 Select **None** in the **Minimum font size** drop-down list.

2 Select the **Allow pages to choose their own fonts, instead of my selections above** check box.

3. Click **OK**.

4. Close the **Content** window.

Page Caching

To set the Internet Explorer page caching options:

Internet Explorer browser>>Tools>>Internet Options

1. Select the **General** tab

2. Click **Settings**.

3. In the **Check for new versions of stored pages** area, select the **Automatically** radio button.

4. Click **OK**.

5. In the **Internet Options** dialog box, click the **Advanced** tab.

6. Scroll down to the **Security** area. Clear the **Do not save encrypted pages to disk** check box.

7. Click **OK**.

To set the Mozilla page caching options:

Mozilla browser>>Edit>>Preferences

1. Click the plus (+) symbol next to **Advanced** to expand the topic.

2. Select **Cache**.

3. In the **Compare the page in the cache to the page on the network** area, select the **Every time I view the page** radio button.

4. Click **OK**.

Temporary Files

Periodically delete temporary files from your system to improve browser performance.

To delete temporary files in Internet Explorer:

Internet Explorer>>Tools>>Internet Options>>General tab

1. Click **Delete Files**.

2 Select the **Delete all offline content** check box.

3 Click **OK**.

4 Click **OK**.

To delete temporary files in Mozilla:

Mozilla browser>>Edit>>Preferences

1 Select the plus (+) symbol next to **Advanced** to expand the topic.

2 Select **Cache**.

3 Click **Clear Cache**.

To delete temporary files in Windows or Linux Firefox:

Firefox browser>>Tools>>Options>>Privacy

1 In the **Private Data** area, click **Settings**. The **Clear Private Data** window appears.

2 Select the **Cache** check box.

3 Click **OK**.

4 Click **Clear Now**.

5 Click **OK**.

To delete temporary files in Mac Firefox:

Firefox menu>>Preferences>>Privacy

1 In the **Private Data** area, click **Settings**. The **Clear Private Data** window appears.

2 Select the **Cache** check box.

3 Click **OK**.

4 Click **Clear Now**.

5 Close the **Privacy** window.

Operating Systems Supported

When Sentriant AG is installed on the dedicated server, the required operating system is also installed on the dedicated server.

The end-user endpoints that can be tested for this release must have one of the following operating systems:

- Mac OS X
  - Mac OS X version 10.3.7 or later.
  - Both the PowerPC and Intel Macintosh computers are supported
- Windows Server 2003
  - Service Pack: SP1
  - Language Support: U.S. English
- Windows 2000
  - Service Pack: SP4
  - Language Support: U.S. English
- Windows XP Home, Windows XP Pro
  - Service Pack: SP1 or SP2
  - Language Support: U.S. English
- Windows ME
  - Language Support: U.S. English

Software Supported

- DHCP
  - Microsoft DHCP Server
- RADIUS Server
  - Microsoft Windows Server 2003 Internet Authentication Service (IAS)
  - FreeRADIUS (included with Sentriant AG)
- Browser Support
  - Management Server
    - Internet Explorer 6.0 or later
    - Mozilla Firefox 1.5 or higher
  - Endpoint
    - Internet Explorer 6.0 or later
    - Mozilla Firefox 1.5 or higher
    - Safari
- Supplicant
  - Windows Supplicant

  - Odyssey (Funk Software/Juniper® Networks) Supplicant

Enforcement Methods Requirements

The following enforcement methods have the following associated requirements:

- Sentriant AG cannot test multiple endpoints behind a Network Address Translation (NAT) server.
- DHCP (all modes)
  - Sentriant AG must be inline with the DHCP server.
  - Sentriant AG supports Microsoft's DHCP server and ISC.
  - Sentriant AG does not support PXE boot with DHCP.
  - Multiple DHCP servers on the same segments must be configured as primary / secondary.
  - Sentriant AG does not enforce Static IPs in DHCP mode.
- DHCP network mode
  - Multinet must be possible.
  - ACLs must be added to the router to create a quarantine area with enough IP address space equivalent to the production LANs.
- DHCP endpoint mode
  - Browsers must be enabled to detect proxy server or static proxy server by host name.
  - If a user has administrative credentials, enforcement can be circumvented.
- Inline mode
  - Only works with VPNs inline with Sentriant AG.
  - The Sentriant AG server must have two NICs integrated onto the motherboard.
- 802.1x
  - All switches must have 802.1x support.
  - Clients must have Windows or Funk supplicants.
  - Specific Windows supplicants tested are EAP, PEAP, MD5 challenge.
  - Switches must send Calling_Station_ID and NAS_Port Radius attributes.
- 802.1x RADIUS server support
  - Proxy method
    - FreeRADIUS on Linux
    - Microsoft IAS on Windows
    - Cisco ACS on Windows 2003 Server
  - Plug-in method
    - FreeRADIUS on Linux
    - Microsoft IAS on Windows

1 Installing Sentriant AG

You have two installation options:

- Install Sentriant AG for the first time (see "Installing Sentriant AG for the First Time")
- Upgrade to a newer version of Sentriant AG (see "Upgrading Sentriant AG to a Newer Version" on page 24)

Installing Sentriant AG for the First Time

For first-time installations, use the install CD. Create an install CD from an International Organization for Standardization (ISO) image downloaded from the Extreme Networks, Inc. Web site. The installation process loads both the Sentriant AG application and the custom, hardened operating system (OS) on which Sentriant AG runs.

NOTE

If you already have a CD, skip to "Installing Sentriant AG" on page 3.

This section covers the following tasks:

- "Downloading the New Install ISO Image" on page 1
- "Creating the Installation CD from the Sentriant AG Download" on page 2
- "Installing Sentriant AG" on page 3

Downloading the New Install ISO Image

After you download the ISO image, create a CD (see "Creating the Installation CD from the Sentriant AG Download" on page 2), and then perform the installation from the CD (see "Installing Sentriant AG" on page 3).

To download the new install ISO using Internet Explorer:

Internet Explorer (IE) or other browser

1 Locate a computer that has a browser installed and is connected to the Internet.

2 Open a browser window and navigate to the following URL:

http://download.sentriantag.extremenetworks.com/SentriantAG-current.iso

The approximate file size is 450 MB.

3 A pop-up window appears with instructions about saving the file, click **Save**.

4 A pop-up window appears instructing you to select a directory in which to save the file. Navigate to a location that you will remember when it is time to create the install CD. Click **Save**.

5 The download window appears, showing the status of the download process. This download can take a lot of time, depending on your connection speed.

6 After you download the file (ISO image), you need to create a CD (see "Creating the Installation CD from the Sentriant AG Download" on page 2), and then you can use that CD to install the Sentriant AG software (see "Installing Sentriant AG" on page 3).

NOTE

Downloading an ISO image file and creating an installation CD is not the same process as just copying a file to a CD.

Creating the Installation CD from the Sentriant AG Download

NOTE

If you already have a Sentriant AG installation CD, go to "Installing Sentriant AG" on page 3.

You must have a CD to install Sentriant AG. This section describes how to create one from the downloaded ISO image.

To create the Sentriant AG installation CD:

1 *For Windows*:

a Most current CD-burning software supports creating CDs from ISO images. Open the ISO file with your CD-burning software. If it recognizes the ISO file, proceed with the CD-burning process.

or

b Right-click on the ISO file and choose **Open with**>>**Choose program** and select your CD-burning software. After your CD program launches, create the CD using the typical procedures.

NOTE

*A Free CD-burning application you can try is CDBurnerXP Pro (*http://www.cdburnerxp.se*)*

2 *For Linux*:

Most Linux systems include the `cdrecord` command; however, `cdrecord` syntax varies depending on the specific distribution. Consult your documentation for the correct syntax for your version.

For example:

```
cdrecord -v speed=8 dev=0,0,0 /tmp/imagefile.iso
```

Where `8` is the speed of your burner, and `/tmp/imagefile.iso` is the path and file name of the ISO file you wish to copy.

Installing Sentriant AG

When you install the Sentriant AG software for the first time, you need to put the Sentriant AG CD directly into the computer that will be the Sentriant AG server (MS or ES). You cannot install any other software on this computer. Installing the Sentriant AG software also installs the operating system (OS) that Sentriant AG uses. This OS is *hardened* making it very secure.

CAUTION

Installing third-party software on the Sentriant AG server is not supported. If you install additional software on the Sentriant AG server, you will have to remove it in order to troubleshoot any Sentriant AG issues, and it will likely be partially or fully overwritten during Sentriant AG release upgrades or patch installs, compromising the third-party software functionality. Additionally, installing third-party software and/or modifying the Sentriant AG software may violate your license agreement. Please refer to the Extreme Networks, Inc. EULA, which can be found in the Sentriant AG Users Guide.

There are two scenarios for Sentriant AG installation:

- **Single-server installation**—Install Sentriant AG as a single-server installation, where the MS and the ES are both on the same server. The ES is automatically joined to an Enforcement cluster. The high availability (HA) and load balancing (LB) functions are not available with this installation option.
- **Multiple-server installation**—Install Sentriant AG as a multiple-server installation where the MS and the ES or ESs are on different servers. One or more ESs are joined to a specified Enforcement cluster in the user interface. You must have two or more ESs joined to an Enforcement cluster for HA or LB functionality.

After you install Sentriant AG, you need to use a computer (other than the MS or ES) with a browser for configuration and daily operation tasks.

See the *Sentriant AG Users Guide* for more information on HA and LB.

To install Sentriant AG:

1 Locate and verify the server hardware (see “Locating and Verifying Server Hardware” on page 4).

2 Locate the information required during the install process (see “Information Required During Installation” on page 5).

3 Install the software:

   a Install single-server MS/ES software (see “Creating a Single-server Installation” on page 6), or

   b Install multiple-server MS software and ES software (see “Creating a Multiple-server Installation” on page 13)

4 Log in to the Sentriant AG MS.

5 For multiple-server installations:

a Create clusters (see "Creating an Enforcement Cluster" on page 19).

b Add enforcement servers to defined clusters (see"Adding an ES to a Cluster" on page 22)

6 Configure Sentriant AG (see the *Sentriant AG Version 5.2 Users Guide*).

Locating and Verifying Server Hardware

To verify the server requirements:

1 Locate the computer you will be using for the Sentriant AG server.

2 Verify that this computer has the following:

a **Processor** – Intel Dual Core (Core 2 Duo/Xeon 5100 series)

- **Linux** – To list CPU-related information to the screen on a Linux computer, enter the following at the command line:
  ```
  cat /proc/cpuinfo | more
  ```
  Press the space bar to page down through the listed information
- **Windows** – From the desktop, right click on **My Computer** and select **Properties**. Select the **General** tab.

b **Processor speed** – 1.86 GHz (or greater).

- **Linux** – To list CPU-related information to the screen on a Linux computer, enter the following at the command line:
  ```
  cat /proc/cpuinfo | more
  ```
  Press the space bar to page down through the listed information.
- **Windows** – From the desktop, right click on **My Computer** and select **Properties**. Select the **General** tab.

c **Memory** – 2 GB RAM

- **Linux** – To list memory-related information to the screen on a Linux computer, enter the following at the command line:
  ```
  dmesg | grep Memory
  ```
  The number returned to the right of the / is the total memory.
- **Windows** – From the desktop, right click on **My Computer** and select **Properties**. Select the **General** tab.

d **Disk space** – 80 GB SATA disk drive

- **Linux** – To list disk-related information to the screen on a Linux computer, enter the following at the command line:

  For IDE drives:
  ```
  fdisk -l /dev/hda | more
  ```

  For SCSI drives:
  ```
  fdisk -l /dev/sda | more
  ```

  Press the space bar to page down through the listed information. If you don't know the drive type, just pick one of the above commands and enter it. If you don't have that type of drive, nothing will be returned.
- **Windows** – From the desktop, double-click on **My Computer**.

e **Ethernet cards**—You must know the quarantine (deployment) method you are going to use when setting up your network, as each method has the following specific Ethernet card requirements:

Single-server installation—When the MS and ES are installed on the same server, you need two Ethernet cards.

Multiple-server installation—When the MS and ES are installed on multiple servers, you need one Ethernet card on the MS, and the following number of Ethernet cards for each ES:

Inline—You need two Ethernet cards on each ES
DHCP—You need two Ethernet cards on each ES
802.1x—You need one Ethernet card on each ES

- **Linux**—To list Ethernet card information to the screen on a Linux computer, enter the following at the command line:

```
ifconfig
```

- **Windows**—To list Ethernet card information to a DOS (cmd) window on a Windows computer, enter the following at the command line:

```
ipconfig
```

f **CD ROM drive—**This drive can be a read-only drive and is used for first-time installation.

NOTE

For more information about deployment options, see "Deployment Flexibility" on page 1.

CAUTION

Make sure that your Ethernet cards are 10/100/1000 (Intel) server-class NICs. Inferior class network cards do not work at all, or work intermittently. You can get the best results from the Intel PRO-series NICs.

Information Required During Installation

You will be asked for the following information during the installation process (use the "Installation and Configuration Check List" on page 1 for easy reference):

- **Static IP address—**The IP address for each server you will use (both MS and ESs). For example: 10.0.16.180. You must have a static (always the same) (not dynamic—can be different every time) IP address to use for each server.
- **Netmask (Network mask)—**A number that tells how much of the IP address is reserved for the network (255) and how much is reserved for the host (0). This must be defined when servers create subnetworks as part of the installation process. For example: 255.255.0.0.
- **Default gateway IP address—**The IP address of your Internet connection—the IP address of the network endpoint that knows how to route packets outside of your local network. For example 10.0.16.1.

  To find the current Default Gateway:
  Linux – Enter `route -n` at the command line
  Windows - Enter `ipconfig` at the command line

NOTE

Your system may require a different gateway. Check with your network administrator if you have problems or are unsure of which gateway IP address to use.

- **Primary nameserver IP address (DNS server)—**The IP address of the server that you use to convert hostnames to IP addresses. For example: 204.74.112.1.

  To find the current DNS server:
  Linux – Look in the `/etc/resolv.conf` file for the `nameserver` entry.
  Windows – Enter `ipconfig /all` at the command line

  If you use secondary and tertiary nameservers, you will be asked for those IP addresses as well.
- **Sentriant AG hostname —**The names you give your Sentriant AG servers (MS and ESs). Select names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

NOTE

The Sentriant AG hostnames must be the fully qualified domain names (FQDN). The FQDN includes the host and the domain name—including the top-level domain. For example, waldo.mycompany.com.

- **Time zone—**The time zones where your Sentriant AG servers are located. The time zones must be specified for each MS and each ES.
- **Sentriant AG server root password—**The passwords you give to your Sentriant AG servers (MS and ESs) when logging in as the `root` user. **Note:** This is *not* the Sentriant AG user interface administrator password.
- **Installation type—**The type is either MS or ES for multiple-server installations, or Both for single-server installations.
- **NTP server IP—**The IP address you use for your Network Time Protocol (NTP) server

Creating a Single-server Installation

To install the MS and ES on a single server:

1 Locate the server you are using for the Sentriant AG installation.

2 Insert the Sentriant AG CD into the dedicated server and reboot (for example by pressing [Ctrl]+[Alt]+[Delete] or an appropriate method of reboot). Once the server reboots, the boot prompt screen appears (Figure 1).

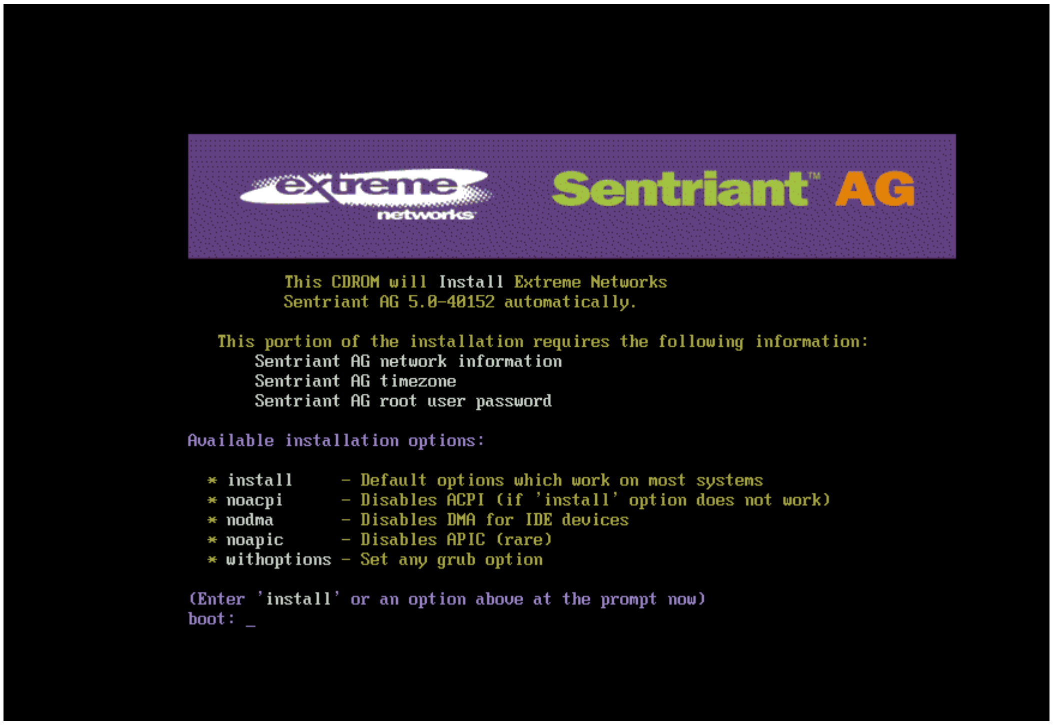
WARNING!

The Sentriant AG installation CD automatically reformats the hard drive on the host machine, erasing all existing data. Do not continue if you need any information that is stored on the hard drive! To abort the installation, press [Ctrl]+[Alt]+[Delete].

NOTE

If the dedicated server is not configured to boot from the CD drive, edit the basic input/output system (BIOS) options as described in your server's documentation.

Figure 1: Install Screen, Boot Prompt



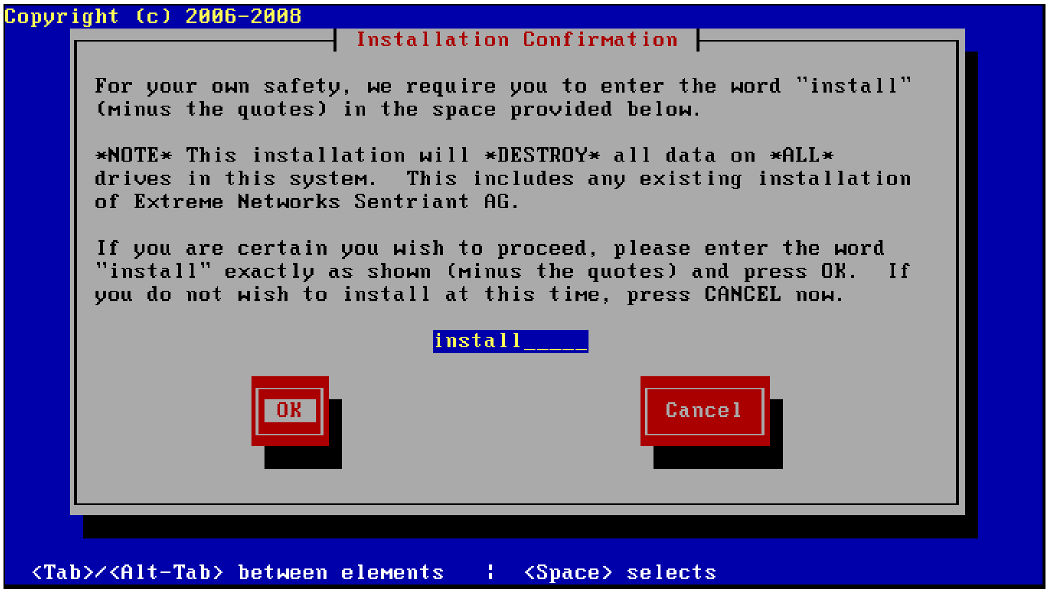
```
        This CDROM will Install Extreme Networks
        Sentriant AG 5.0-40152 automatically.

   This portion of the installation requires the following information:
       Sentriant AG network information
       Sentriant AG timezone
       Sentriant AG root user password

Available installation options:

  * install     - Default options which work on most systems
  * noacpi      - Disables ACPI (if 'install' option does not work)
  * nodma       - Disables DMA for IDE devices
  * noapic      - Disables APIC (rare)
  * withoptions - Set any grub option

(Enter 'install' or an option above at the prompt now)
boot: _
```

3 At the boot prompt, type one of the following:

- `install`—This is the default option that works on most systems.
- `noacpi`—If your system hangs shortly after install is entered, use this option which disables the [Advanced Configuration and Power Interface (ACPI)] allowing the Sentriant AG system to use the chroot command.
- `nodma`—If your system (such as some Compaq/HP systems) has problems using [Direct Memory Access (DMA)] to chip memory, this option disables DMA for the IDE subsystem.
- `noapic`—If your system BIOS has an upgrade to fix the Advanced Programmable Interrupt Controller (APIC)] and the system continues to hang shortly after install is entered, use this option which disables the APIC. This tells the kernel to not make use of any IOAPICs that may be present in the system.
- `withoptions`—If your system has problems not listed above, use this option to specify that No additional kernel parameters are passed to the kernel to allow greater flexibility.

4 Press [Enter]. The **Installation Confirmation** screen appears:.

Figure 2: Install Screen, Installation Confirmation



```
Copyright (c) 2006-2008
                    Installation Confirmation

   For your own safety, we require you to enter the word "install"
   (minus the quotes) in the space provided below.

   *NOTE* This installation will *DESTROY* all data on *ALL*
   drives in this system.  This includes any existing installation
   of Extreme Networks Sentriant AG.

   If you are certain you wish to proceed, please enter the word
   "install" exactly as shown (minus the quotes) and press OK.  If
   you do not wish to install at this time, press CANCEL now.

                          install_____
```

5 On the **Installation Confirmation** screen, type `install` and select **OK**. The **Network Configuration for eth0** screen appears.

NOTE

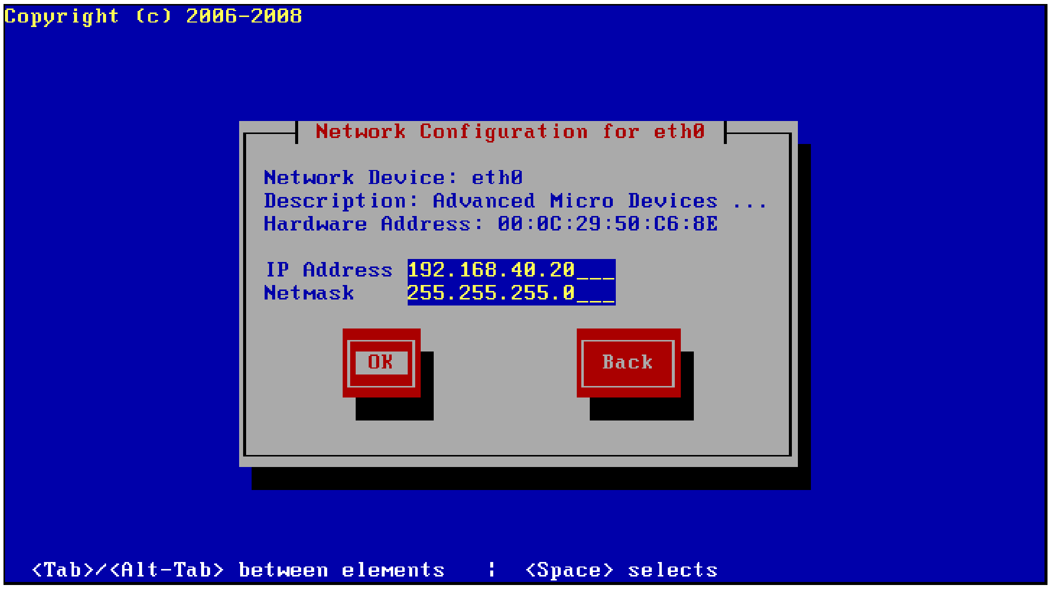
Use the [Tab], [spacebar], and [Enter] keys to navigate between fields and make selections on the install screens.

6 On the **Network Configuration for eth0** screen, enter the IP address of the Sentriant AG MS/ES installation, as shown in Figure 3. The **Netmask** value is prepopulated; edit the **Netmask** value if necessary.

NOTE

You must use static IP addresses for Sentriant AG servers. Sentriant AG servers cannot receive DHCP IP addresses.

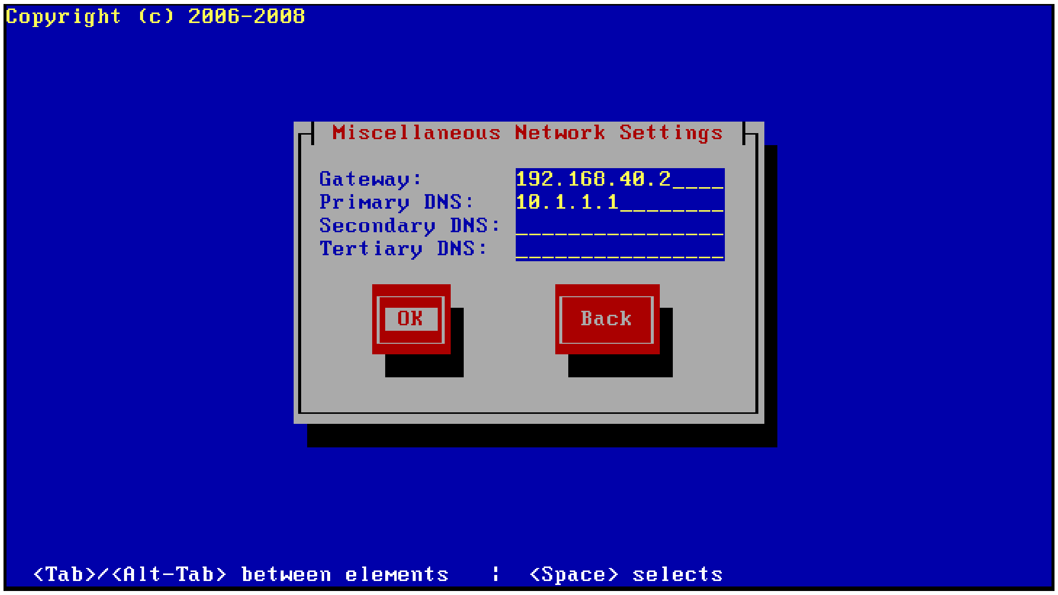
Figure 3: Install Screen, Network Configuration for eth0



```
Copyright (c) 2006-2008

Network Configuration for eth0

Network Device: eth0
Description: Advanced Micro Devices ...
Hardware Address: 00:0C:29:50:C6:8E

IP Address 192.168.40.20___
Netmask    255.255.255.0___

<Tab>/<Alt-Tab> between elements   |  <Space> selects
```

7 Select **OK**. The **Miscellaneous Network Settings** screen appears:

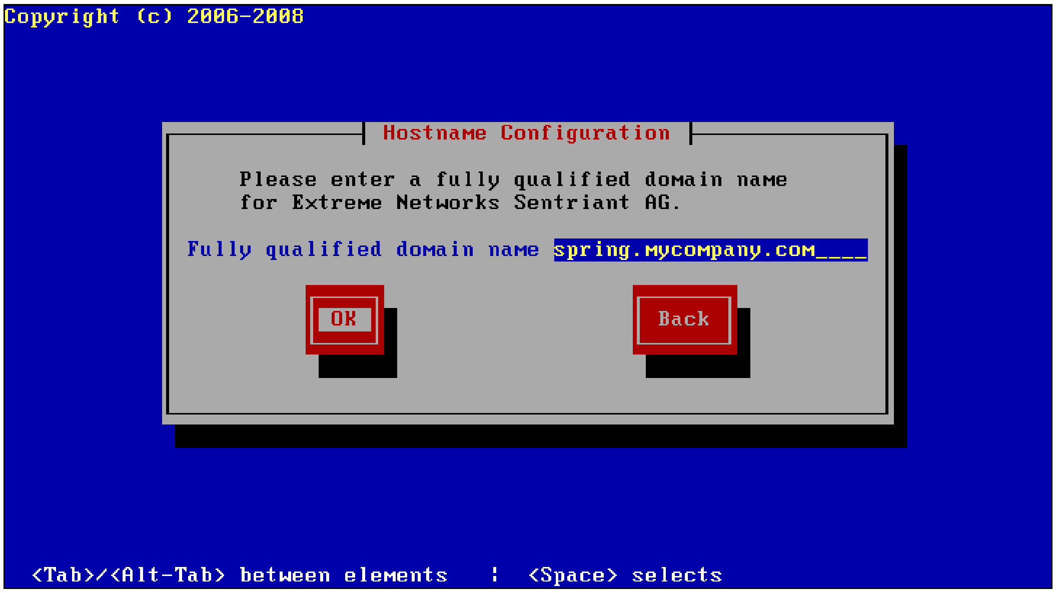
Figure 4: Install Screen, Miscellaneous Network Settings



```
Copyright (c) 2006-2008

Miscellaneous Network Settings

Gateway:        192.168.40.2____
Primary DNS:    10.1.1.1________
Secondary DNS:  ________________
Tertiary DNS:   ________________

<Tab>/<Alt-Tab> between elements   |  <Space> selects
```

8 On the **Miscellaneous Network Settings** screen, enter the **Gateway** and **Primary DNS**, (and **Secondary DNS** and **Tertiary DNS** if you use them). Select **OK**. The **Hostname Configuration** screen appears:

Figure 5: Install Screen, Hostname Configuration



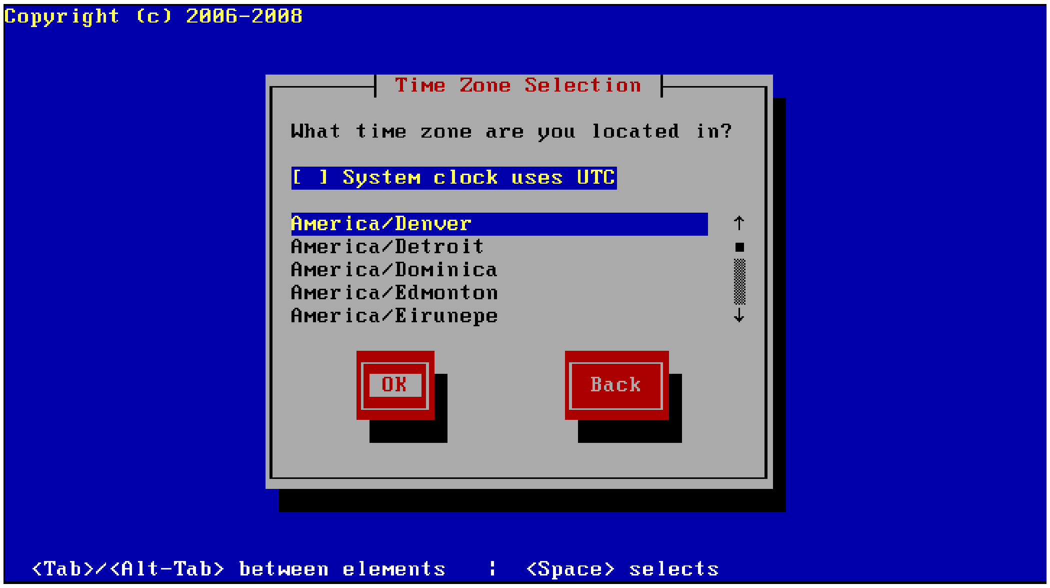
```
Copyright (c) 2006-2008

Hostname Configuration

Please enter a fully qualified domain name
for Extreme Networks Sentriant AG.

Fully qualified domain name spring.mycompany.com____

<Tab>/<Alt-Tab> between elements   |  <Space> selects
```

9 On the **Hostname Configuration** screen, enter the hostname. This name must be the fully qualified domain name (FQDN). Select **OK**. The **Time Zone Selection** screen appears:

NOTE

Select simple names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

Figure 6: Install Screen, Time Zone Selection



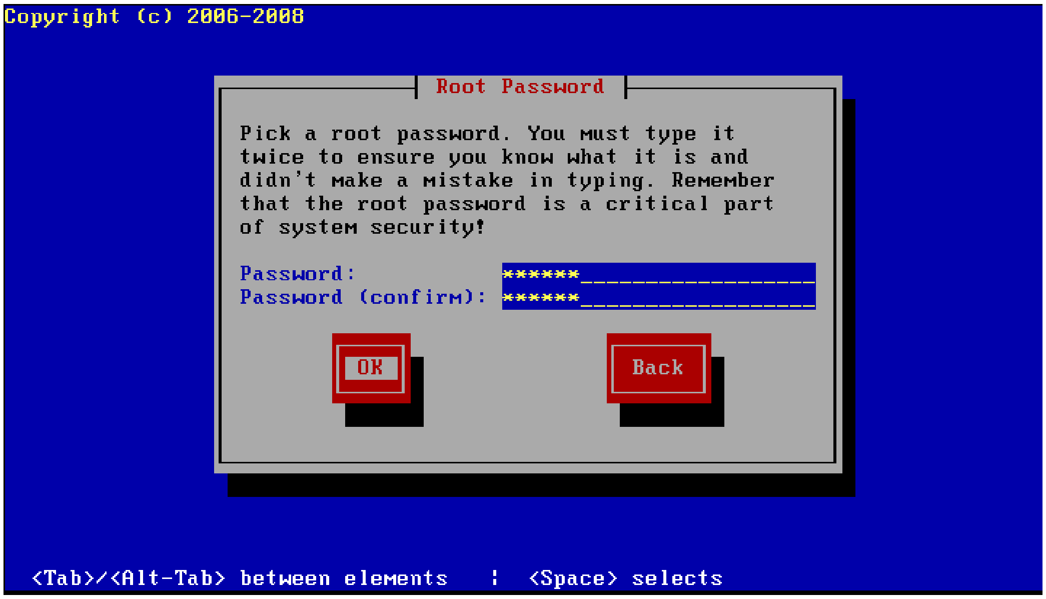
```
Copyright (c) 2006-2008

Time Zone Selection

What time zone are you located in?

[ ] System clock uses UTC

America/Denver
America/Detroit
America/Dominica
America/Edmonton
America/Eirunepe

<Tab>/<Alt-Tab> between elements   |  <Space> selects
```

10 On the **Time Zone Selection** screen, select the time zone. Select **OK**. The **Root Password** screen appears:

NOTE

Make sure that you select a root password that is easy for you to remember but difficult for others to guess.

Figure 7: Install Screen, Root Password



Copyright (c) 2006-2008

Root Password

Pick a root password. You must type it twice to ensure you know what it is and didn't make a mistake in typing. Remember that the root password is a critical part of system security!

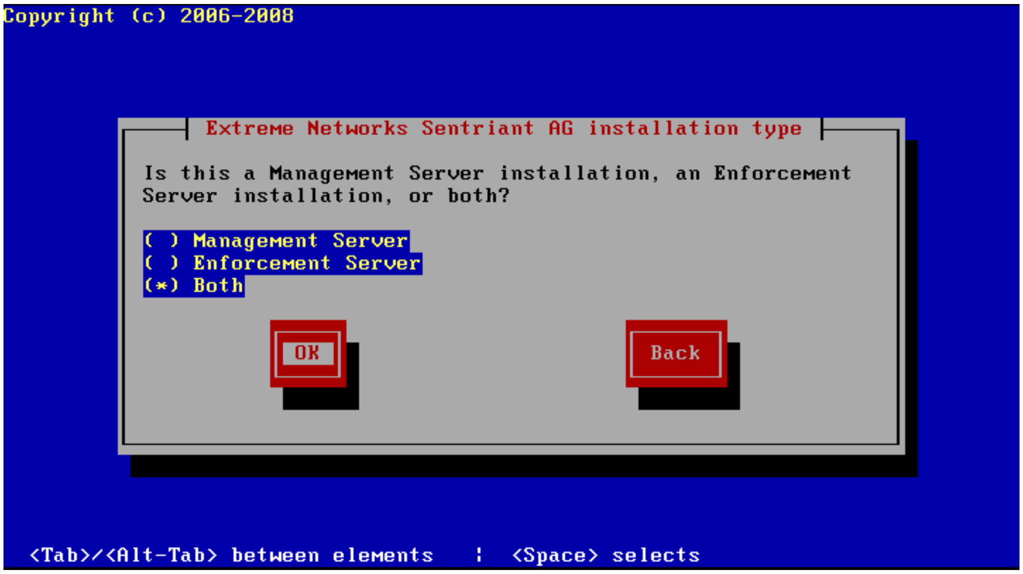
Password: ******

Password (confirm): ******

<Tab>/<Alt-Tab> between elements | <Space> selects

11 On the **Root Password** screen, enter a root password for the Sentriant AG server. Enter a secure password that you can remember, and retype the password to confirm it. Select **OK**. The **Extreme Networks, Inc. Sentriant AG installation type** screen appears:

Figure 8: Install Screen, Installation Type



Copyright (c) 2006-2008

Extreme Networks Sentriant AG installation type

Is this a Management Server installation, an Enforcement Server installation, or both?

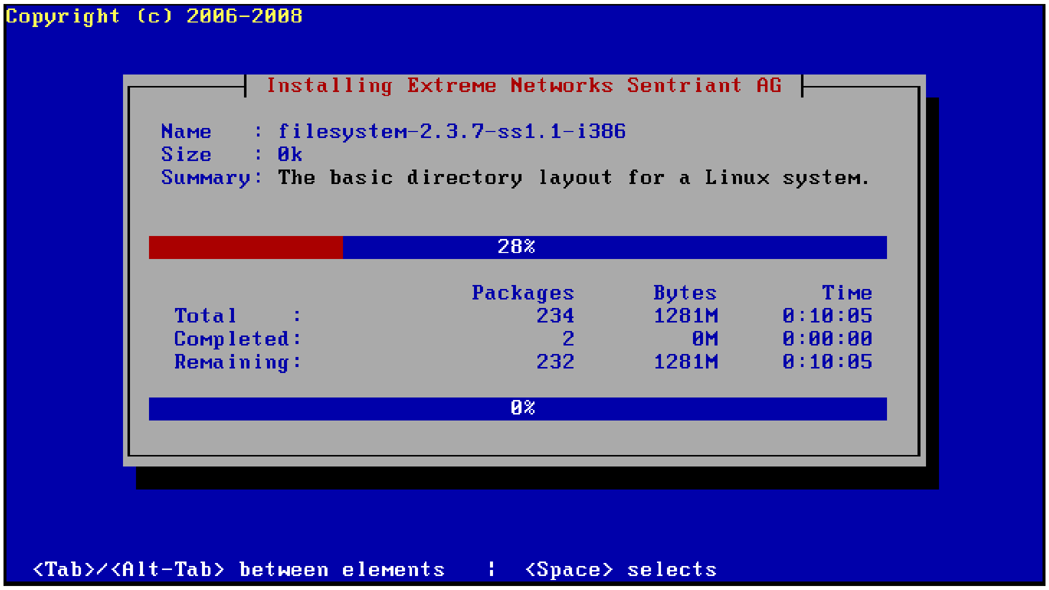
( ) Management Server
( ) Enforcement Server
(*) Both

<Tab>/<Alt-Tab> between elements | <Space> selects

12 On the **Extreme Networks, Inc. Sentriant AG installation type** screen, select **Both**.

13 Select **OK**. The **Installation progress** screen appears (Figure 9).

Figure 9: Install Screen, Installation Progress



```
Copyright (c) 2006-2008

          ┤ Installing Extreme Networks Sentriant AG ├

            Name    : filesystem-2.3.7-ss1.1-i386
            Size    : 0k
            Summary: The basic directory layout for a Linux system.

                                  28%

                                 Packages     Bytes       Time
             Total     :              234     1281M    0:10:05
             Completed:                 2        0M    0:00:00
             Remaining:               232     1281M    0:10:05

                                   0%

  <Tab>/<Alt-Tab> between elements   |  <Space> selects
```

14 Wait. Installation can take a few minutes.

15 When installation is complete, remove the CD.

NOTE

If the server reboots before you remove the CD, the boot prompt appears again. Remove the CD and reboot the server to start Sentriant AG.

16 The server reboots and starts Sentriant AG.

17 Log in to the Sentriant AG server and perform the initial configuration as described in "Initial Configuration" on page 14.

Creating a Multiple-server Installation

To install the MS and ES on different servers:

1 Install the MS software:

a Perform the steps described in "Creating a Single-server Installation": step 1 on page 6 through step 11 on page 12. The **Extreme Networks, Inc. Sentriant AG installation type** screen appears (Figure 8 on page 12).

b Select **Management server.**

c Select **ok**. The **Installation progress** screen appears (Figure 9 on page 13).

- **d** Wait. Installation can take a few minutes.
- **e** When installation is complete, remove the CD.

NOTE

If the server reboots before you remove the CD, the boot prompt appears again. Remove the CD and reboot the server to start Sentriant AG.

- **f** The server reboots and starts Sentriant AG.

2 Install the ES software:

- **a** Perform the steps described in "Creating a Single-server Installation": step 1 on page 6 through step 11 on page 12. The **Extreme Networks, Inc. Sentriant AG installation type** screen appears (Figure 8 on page 12).
- **b** Select **Enforcement server.**
- **c** Select **ok**. The **Installation progress** screen appears (Figure 9 on page 13).
- **d** Wait. Installation can take a few minutes.
- **e** When installation is complete, remove the CD.

NOTE

If the server reboots before you remove the CD, the boot prompt appears again. Remove the CD and reboot the server to start Sentriant AG.

- **f** The server reboots and starts Sentriant AG.

3 Add as many ESs as your system requires.

4 Go to "Initial Configuration".

Initial Configuration

NOTE

If you already have endpoints attached to a switch when you install Sentriant AG, you must log in to each switch and send the NAC revalidate command before the endpoint can be tested and routed properly.

To configure the Sentriant AG MS/ES:

1 Log into a different computer with browser software installed. The following browsers are supported for this release:

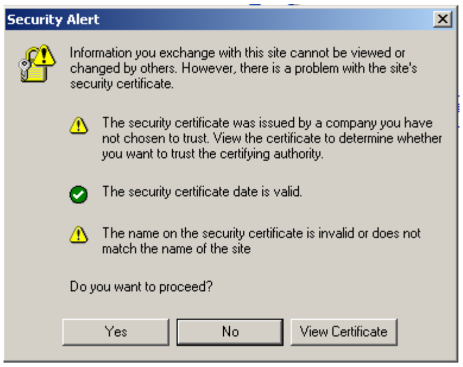
- Windows: IE 6.0 or later, Mozilla Firefox v1.5 or later, Mozilla v1.7

- Linux: Mozilla Firefox v1.5 or later, Mozilla v1.7
- Mac OS X: Mozilla Firefox v1.5 or later

2 Using `https://`, point your browser to the IP address or host name of the Sentriant AG server (for example, `https://10.0.64.25`).

3 You might be prompted with a security alert because Sentriant AG uses a secure communication connection (SSL) (Figure 10). Click **Yes**. The **Accept license agreement** window appears (Figure 11).

Figure 10: Security Alert Window



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

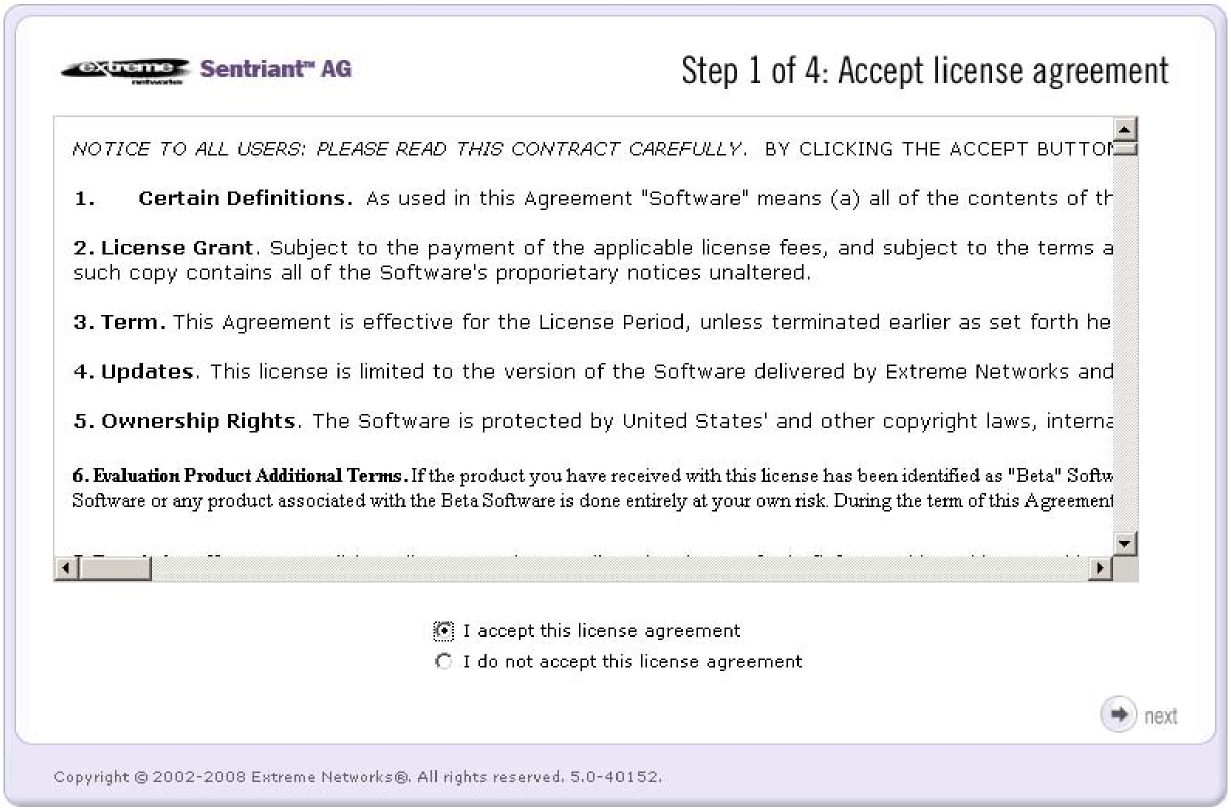
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Figure 11: Accept License Agreement Window



Step 1 of 4: Accept license agreement

NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY CLICKING THE ACCEPT BUTTON

1. **Certain Definitions.** As used in this Agreement "Software" means (a) all of the contents of th

2. **License Grant**. Subject to the payment of the applicable license fees, and subject to the terms a such copy contains all of the Software's proporietary notices unaltered.

3. **Term.** This Agreement is effective for the License Period, unless terminated earlier as set forth he

4. **Updates**. This license is limited to the version of the Software delivered by Extreme Networks and

5. **Ownership Rights**. The Software is protected by United States' and other copyright laws, interna

6. **Evaluation Product Additional Terms.** If the product you have received with this license has been identified as "Beta" Softw Software or any product associated with the Beta Software is done entirely at your own risk. During the term of this Agreement

● I accept this license agreement
○ I do not accept this license agreement

Copyright © 2002-2008 Extreme Networks®. All rights reserved. 5.0-40152.

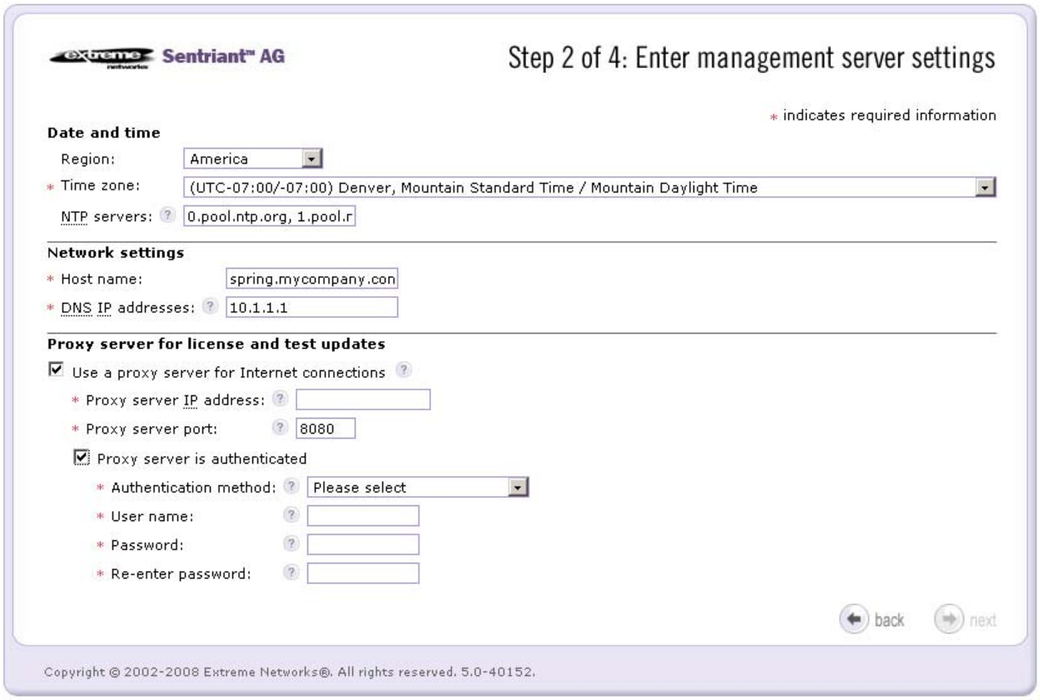
4 Accept the license agreement:

a If you do not wish to accept the license agreement, click **I do not accept this license agreement**, or

b Read the Sentriant AG End-User License Agreement (EULA) and select **I Accept this license agreement.**

c Click **Next**. The **Enter management server settings** window appears.

Figure 12: Enter Management Server Settings Window



Sentriant™ AG

Step 2 of 4: Enter management server settings

* indicates required information

Date and time

Region: America

* Time zone: (UTC-07:00/-07:00) Denver, Mountain Standard Time / Mountain Daylight Time

NTP servers: 0.pool.ntp.org, 1.pool.r

Network settings

* Host name: spring.mycompany.con

* DNS IP addresses: 10.1.1.1

Proxy server for license and test updates

☑ Use a proxy server for Internet connections

* Proxy server IP address:

* Proxy server port: 8080

☑ Proxy server is authenticated

* Authentication method: Please select

* User name:

* Password:

* Re-enter password:

Copyright © 2002-2008 Extreme Networks®. All rights reserved. 5.0-40152.

5 The **Date and time** area is prepopulated with values entered during the initial installation process. Change any of the following if necessary:

- **Region**—Select a region from the drop-down list.
- **Time zone**—Select a time zone from the drop-down list.
- **NTP servers**—Enter one or more Network Time Protocol (NTP) servers, separated by commas. The NTP protocol allows Sentriant AG to synchronize its date and time with other endpoints on your network. For example, `time.nist.gov`.

6 The Network settings area is prepopulated with values entered during the initial installation process. Change any of the following if necessary:

- **Host name**—Enter a Fully Qualified Domain Name (FQDN). For example, `crocus.mycompany.com`.
- **DNS IP address**—Enter one or more DNS resolver IP addresses, separated by commas, semicolons, or spaces. For example, `10.0.16.100,10.0.1.1`.

7 If you use a proxy server, configure it as follows:

a Select the **Use a proxy server for Internet connections** check box. Connecting to the Internet is necessary for updating tests, validating license keys, and sending support packages.

b Enter the IP address of the server that will act as the proxy for Internet connections in the **Proxy server IP address** text box.

c Enter the port used for connecting to the proxy server in the **Proxy server port** text box. For example, `8080`.

d If your proxy server is authenticated, select the **Proxy server is authenticated** check box and enter the following:

1) Select the scheme used to authenticate credentials on the proxy server from the Authentication method drop-down list. The following methods are supported:

Basic—The original and most compatible authentication scheme for HTTP. It is also the least secure because it sends the user ID and password to the server unencrypted.

Digest—Added in the HTTP 1.1 protocol, this scheme is significantly more secure than basic authentication because it never transfers the actual password across the network, but instead uses it to encrypt a `nonce` value sent from the server.

Negotiable—Using this scheme, the client and the proxy server negotiate a scheme for authentication. Ultimately, either the basic or digest scheme will be used.

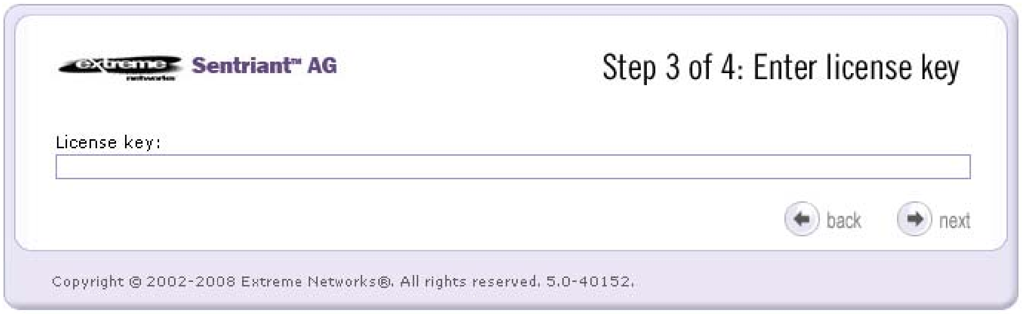
2) Enter the ID of a user account on the proxy server in the **User name** text box.

3) Enter the password of the user account having the ID specified in User ID in the **Password** text box.

4) To help confirm accuracy, type the same password you entered into the **Password** text box in the **Re-enter password** text box.

8 Click **Next**. The **Enter license key** window appears.

Figure 13: Enter License Key Window



Step 3 of 4: Enter license key

License key:

Copyright © 2002-2008 Extreme Networks®. All rights reserved. 5.0-40152.

9 On the **Enter license key** window, in the **License key** field copy and paste your Sentriant AG license key, which was emailed to you as a text file. Click **Next**. The **Create administrator account** window appears.

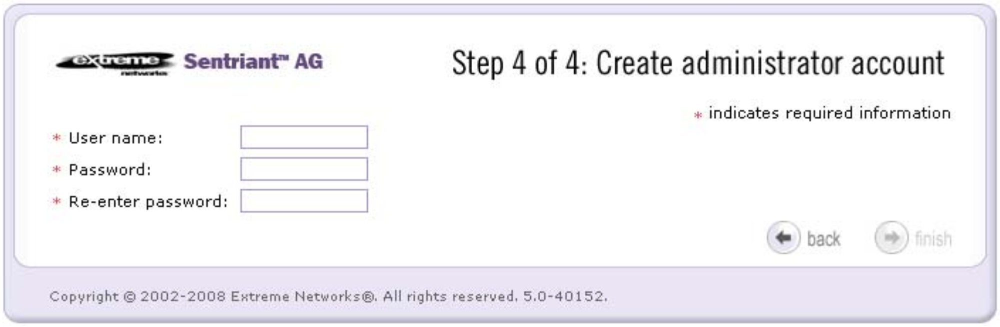
NOTE

An internet connection is required to register/activate the license. The license key is registered to the server once the activation is complete and cannot be moved to another machine without first contacting Technical Assistance Center (TAC).

CAUTION

If you use a proxy server, your license key will not validate from this window unless you have performed step 7 on page 17.

Figure 14: Create Administrator Account Window



Step 4 of 4: Create administrator account

* indicates required information

* User name:

* Password:

* Re-enter password:

Copyright © 2002-2008 Extreme Networks®. All rights reserved. 5.0-40152.

10 On the **Create administrator account** window, create the initial Sentriant AG administrator account. (This is not the same as the server's root account that you created in during installation.)

   a Enter a **User ID** and **Password**. We suggest the password be at least eight characters with a mix of numbers and letters.

   b Click **Finish**.

11 The final step of creating the single-server installation is to configure the default Enforcement cluster. See the *Sentriant AG Users Guide* for instructions on editing Enforcement clusters.

NOTE

In the case of a single-server installation, the MS and ES are on the same server and the ES is automatically joined to a default Enforcement cluster. You can change the name of the Enforcement cluster from the user interface. See the Sentriant AG Users Guide for instructions on editing Enforcement clusters.

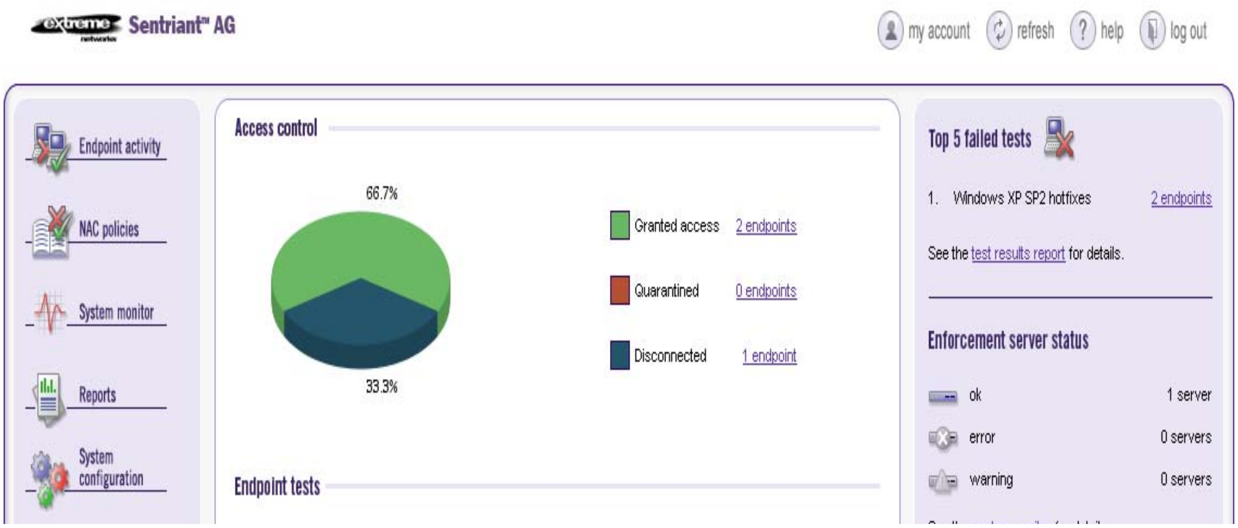
Creating an Enforcement Cluster. When creating a multiple-server installation (the MS and ES are installed on different servers), you must create the clusters before you join the ESs to the cluster.

To create (name) the Enforcement cluster:

1 Using `https://`, point your browser to the IP address or host name of the Sentriant AG server (for example, `https://10.0.64.25`).

2 Using the administrator **User ID** and **Password** you created in step 10 on page 19, log in to the Sentriant AG user interface. The **Sentriant AG Home** window appears:

Figure 15: Sentriant AG Home Window

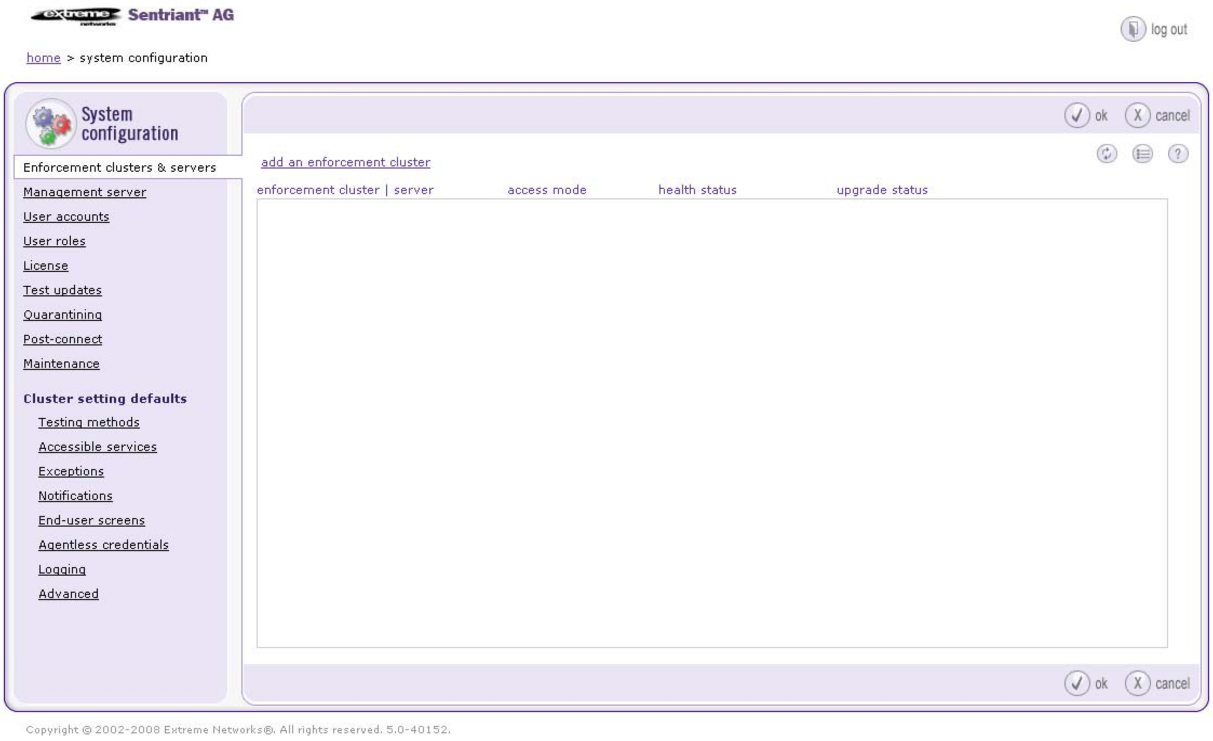


NOTE

The Sentriant AG home window displays the System configuration menu option only for users with administrator permissions. You will see different menu options based on your permissions, which are defined as user roles.

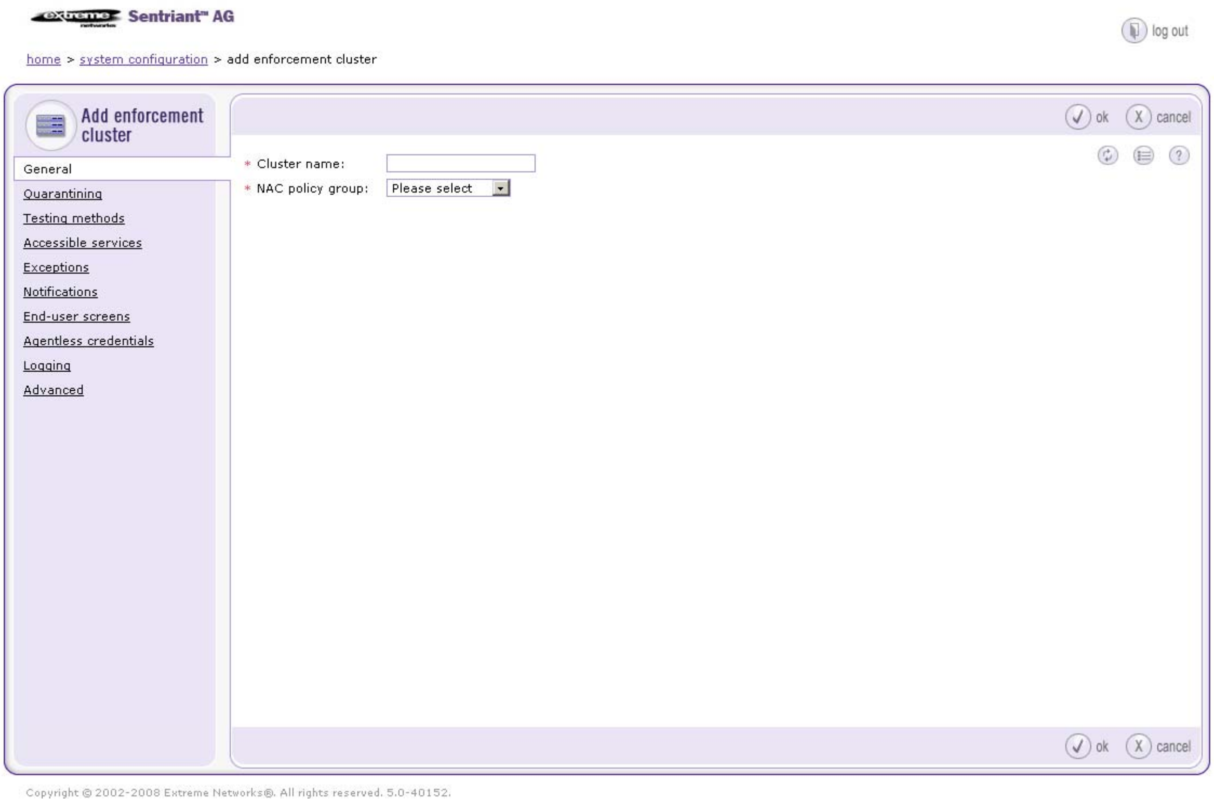
3 Select **System Configuration**. The **System configuration, Enforcement clusters & servers** window appears:

Figure 16: Enforcement Clusters & Servers



4 Click **Add an Enforcement cluster.** The **Add an Enforcement cluster** window appears, with the **General** menu option selected by default.

Figure 17: Add Enforcement Cluster Window



* Cluster name:

* NAC policy group: Please select

Copyright © 2002-2008 Extreme Networks®. All rights reserved. 5.0-40152.

5 In the **Add Enforcement cluster** window, **General** area, enter a name for the cluster in the **Cluster name** field.

6 On the **NAC policy set** drop-down list, select **Default**.

7 Before Sentriant AG is fully functional, you must select the operating parameters for each cluster; however, you do not have to do this now. When you are ready to configure the clusters, refer to the *"Adding a cluster"* section in the *Sentriant AG Users Guide*.

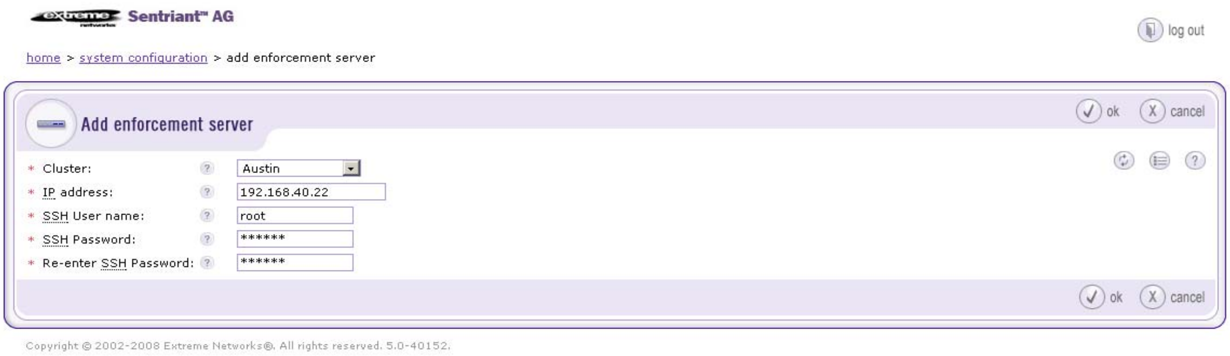
8 Click **ok** to save the cluster and return to the **System configuration** window.

Adding an ES to a Cluster. ***To add an ES to a cluster:***

Home window>>System configuration

1 Click **add an enforcement server**. The **Add enforcement server** window appears:

Figure 18: Add Enforcement Server Window



home > system configuration > add enforcement server

Add enforcement server

* Cluster:	Austin
* IP address:	192.168.40.22
* SSH User name:	root
* SSH Password:	******
* Re-enter SSH Password:	******

Copyright © 2002-2008 Extreme Networks®. All rights reserved. 5.0-40152.

2 Select the cluster name for this enforcement server from the **Cluster** drop-down list.

3 Enter the IP address of this enforcement server in the **IP address** text box.

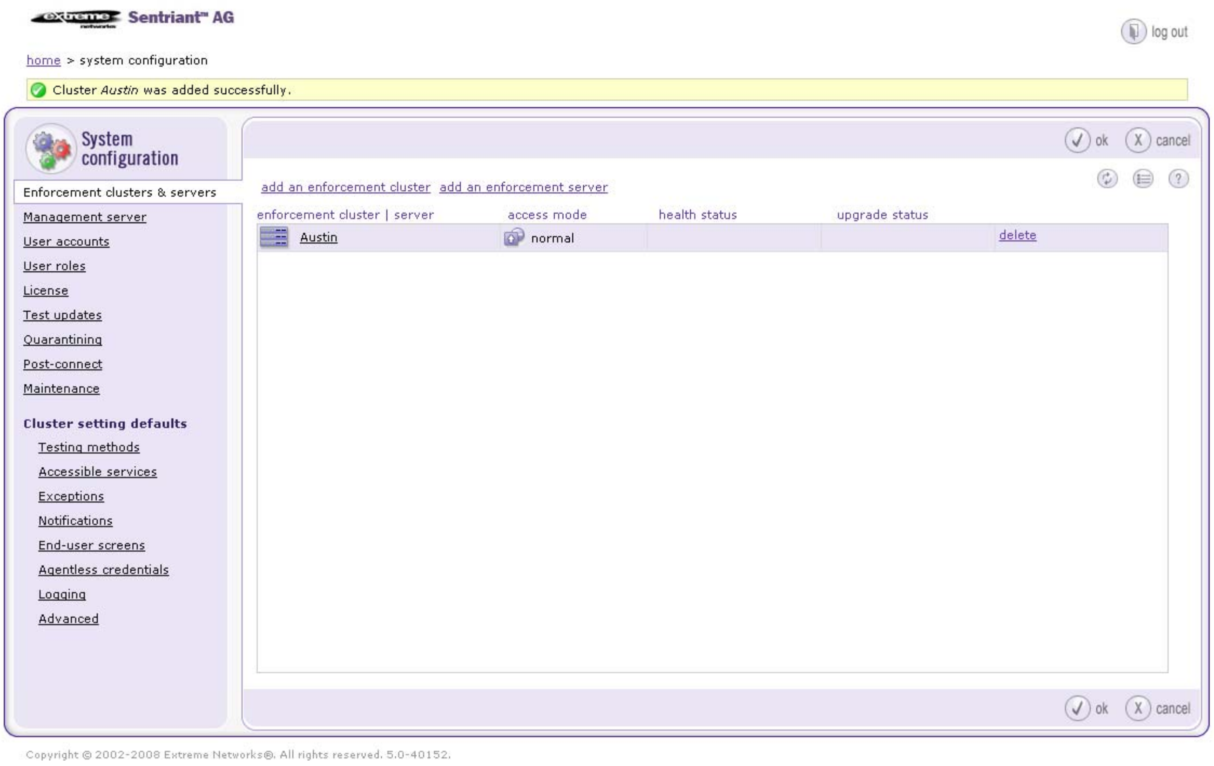
4 The SSH user name must be for an account with sufficient privileges to install certificates. Enter the user name in the **SSH User name** text box.

5 Enter the SSH password for the SSH username account on this enforcement server in the **SSH Password** text box.

6 Re-enter the SSH password for the SSH username account on this enforcement server in the **Re-enter SSH Password** text box.

7 Click **ok** to add the server. A progress window appears. It can take a minute or so to add the server. The **System configuration** window appears showing the server joined to the cluster:

Figure 19: System Configuration, Enforcement Clusters & Servers Window



Cluster *Austin* was added successfully.

enforcement cluster | server	access mode	health status	upgrade status	
Austin	normal			delete

Copyright © 2002-2008 Extreme Networks®. All rights reserved. 5.0-40152.

8 Click **ok** to return to the **Home** window.

CAUTION

The MS must have the same version of software installed as the ES you are adding or you will get an exception error. If you are upgrading an existing system, upgrade the MS, then add new ESs. The upgrade process will automatically upgrade any existing ESs.

Upgrading Sentriant AG to a Newer Version

You can upgrade to Sentriant AG Version 5.2 from v4.x *only* if you are installing a single-server installation (MS and ES on the same server). If you want to install a multiple-server installation, you must do a fresh install.

This section covers the following upgrade options:

- "Upgrading with an Internet Connection" on page 25
- "Upgrading without an Internet Connection" on page 25
- "Downloading the Upgrade ISO Image" on page 29

- "Creating an upgrade CD from the download" on page 29
- "Upgrading from a CD" on page 29

Your upgrade options are as follows:

To upgrade with an Internet connection:

- **v4.x, and prior to v5.0-40103**—Upgrade to v5.0-**40103** from the command line, then upgrade to the current build from the Sentriant AG user interface.
- **v5.0-40103**—Upgrade to the current build from the Sentriant AG user interface.

To upgrade without an Internet connection:

- **v4.x, and prior to v5.0-40103**—Upgrade to v5.0-40103 from the command line, then upgrade to the current build from the Sentriant AG user interface.
  - Create a v5.0-40103 upgrade CD and upgrade from the CD.
  - Create a v5.2-current build upgrade CD and upgrade from the user interface.
- **v5.0-40103**—Upgrade to the current build from the Sentriant AG user interface.
  - Create a v5.2-current build upgrade CD and upgrade from the user interface.

Upgrading with an Internet Connection

Upgrading from Sentriant AG v4.x and Sentriant AG v5.0 prior to v5.0-40103

If you have Sentriant AG 4.x or a Sentriant AG build prior to v5.0-40103, you must first upgrade to Sentriant AG 5.0-40103 from the command line (see "Upgrading from the Command Line" on page 26), then you can install the current version upgrade from the user interface (see "Upgrading from the Sentriant AG User Interface" on page 27).

Upgrading from v4.x is supported only if you are creating a single-server installation where the Management server (MS) and Enforcement server (ES) are on the same physical server.

Upgrades from 4.x to a distributed system (separate MS and ESs) are not supported.

Upgrading from Sentriant AG v5.0-40103 or later

You can upgrade from Sentriant AG 5.0-40103 from the user interface (see "Upgrading from the Sentriant AG User Interface" on page 27).

Upgrading without an Internet Connection

Upgrading from Sentriant AG v4.x and Sentriant AG v5.0 prior to v5.0-40103

If you have Sentriant AG 4.x or a Sentriant AG build prior to v5.0-40103, you must first upgrade to Sentriant AG 5.0-40103 from the command line, then you can install the current version upgrade from the user interface.

Upgrading from v4.x is supported only if you are creating a single-server installation where the Management server (MS) and Enforcement server (ES) are on the same physical server.

Upgrades from 4.x to a distributed system (separate MS and ESs) are not supported.

To create the installation CDs for upgrading with no Internet connection:

1 Create the v5.0-40103 install CD: See "Downloading the Upgrade ISO Image" on page 29 for instructions on downloading the ISO; however, use the following link instead of the one listed:

   http://download.sentriantag.extremenetworks.com/sentriantag-5.0-40103.iso

2 Perform the steps listed in "Creating an upgrade CD from the download" on page 29 and "Upgrading from a CD" on page 29 to upgrade to v5.0-40103 from a CD.

3 Create a v5.2-current build install CD: See "Downloading the Upgrade ISO Image" on page 29 for instructions on downloading the ISO. This time, use the link provided.

4 Perform the steps listed in "Creating an upgrade CD from the download" on page 29 and "Upgrading from a CD" on page 29 to upgrade to v5.2-current build from a CD.

Upgrading from Sentriant AG v5.0-40103 or later

You can upgrade from Sentriant AG 5.0-40103 from the user interface after you create a v5.2-current build CD.

To create the installation CDs for upgrading with no Internet connection:

1 Create a v5.2-current build install CD: See "Downloading the Upgrade ISO Image" on page 29 for instructions on downloading the ISO. Use the link provided.

2 Perform the steps listed in "Creating an upgrade CD from the download" on page 29 and "Upgrading from a CD" on page 29 to upgrade to v5.2-current build from a CD.

If you are upgrading from any other build, please contact Technical Assistance Center (TAC) (support@extremenetworks.com) for assistance.

Upgrading from the Command Line

To download the Sentriant AG upgrade directly from the Linux command line:

NOTE

You cannot upgrade from v5.0-40103 or later to the current build from the command line. You must upgrade from the user interface.

1 Use secure socket shell (SSH) to access the Sentriant AG device using an SSH client such as PuTTY or log in to the console directly. You can download PuTTY from the following location:

   http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

2 Log in as user `root` using the password you set during installation.

3 Change to the `root` home directory:

```
cd /root
```

4 **Optional**—If you need to upgrade through a proxy server, enter the following command:

```
export http_proxy=<server-name-or-ip-address>:<port-number>
```

5 Enter the following commands at the command prompt:

```
wget -N http://download.sentriantag.extremenetworks.com/SentriantAG/Upgrade.py
chmod 755 Upgrade.py
```

6 Enter the upgrade command:

   Upgrading with an internet connection:

```
 ./Upgrade.py
```

   Upgrading from a CD:

```
/Upgrade.py --cdrom
```

7 On the upgrade description screen, enter **yes**. The upgrade process appears on the screen.

8 Wait. The upgrade can take a long time.

9 If the server needs to reboot, it will ask you to do that by pressing `[Ctrl]+[Alt]+[Del]`:

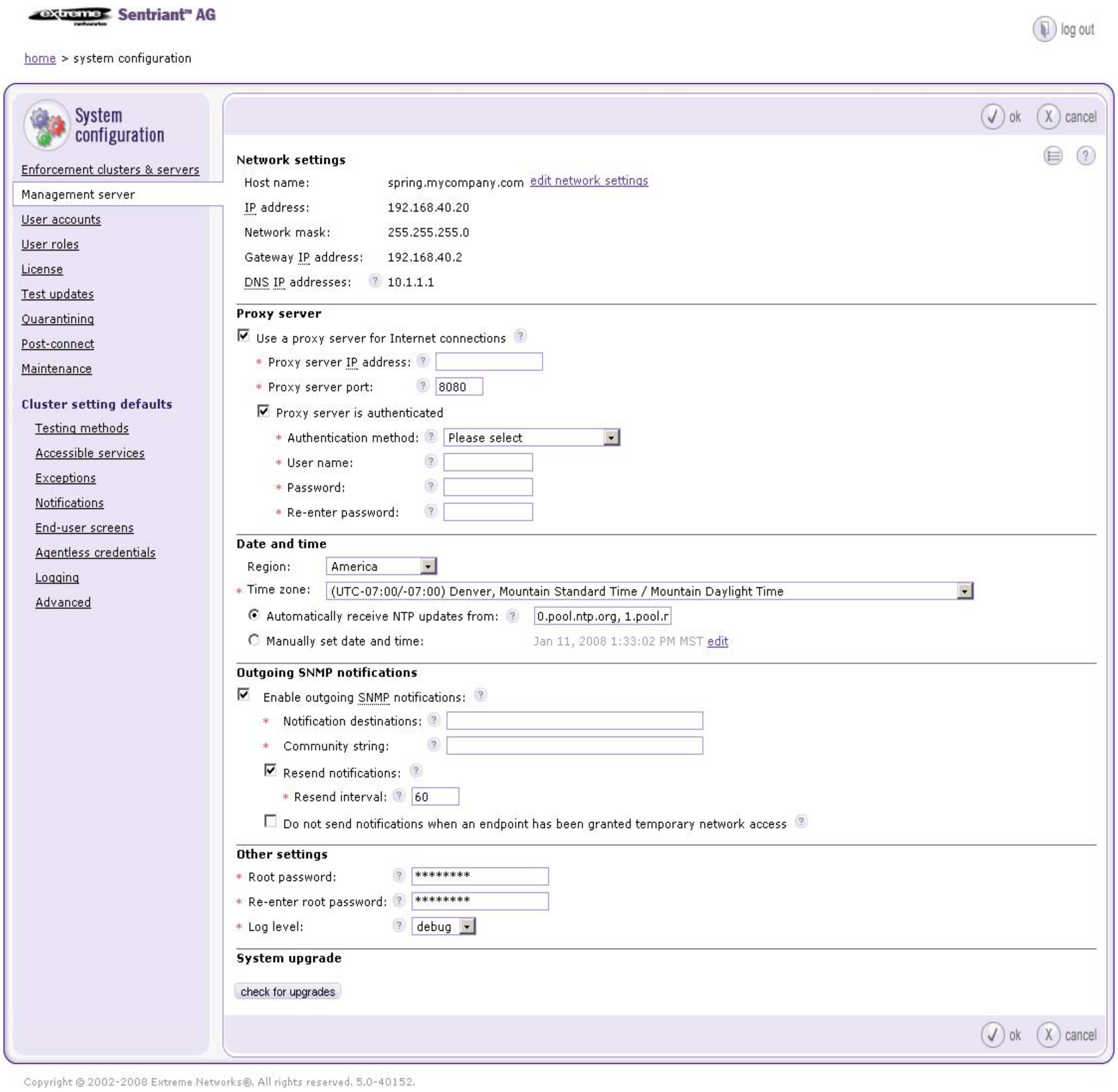
```
The system MUST be rebooted before it can be used again.
Please note that some error messages will be displayed
when the system is rebooted. This is normal and will
be corrected when the system is rebooted.

Please reboot the system NOW by pressing [Ctrl]+[Alt]+[Del].
```

Upgrading from the Sentriant AG User Interface

To upgrade Sentriant AG from the user interface:

Home window>>System configuration>>Management server

Figure 20: System Configuration Window, Management Server Option



Network settings

Host name: spring.mycompany.com edit network settings

IP address: 192.168.40.20

Network mask: 255.255.255.0

Gateway IP address: 192.168.40.2

DNS IP addresses: 10.1.1.1

Proxy server

☑ Use a proxy server for Internet connections

* Proxy server IP address:

* Proxy server port: 8080

☑ Proxy server is authenticated

* Authentication method: Please select

* User name:

* Password:

* Re-enter password:

Date and time

Region: America

* Time zone: (UTC-07:00/-07:00) Denver, Mountain Standard Time / Mountain Daylight Time

● Automatically receive NTP updates from: 0.pool.ntp.org, 1.pool.r

○ Manually set date and time: Jan 11, 2008 1:33:02 PM MST edit

Outgoing SNMP notifications

☑ Enable outgoing SNMP notifications:

* Notification destinations:

* Community string:

☑ Resend notifications:

* Resend interval: 60

□ Do not send notifications when an endpoint has been granted temporary network access

Other settings

* Root password: ********

* Re-enter root password: ********

* Log level: debug

System upgrade

check for upgrades

1 Click **check for upgrades** in the **System upgrade** area. A progress window appears.

2 A status window appears indicating if upgrades are available.

a If no upgrades are available:

1) Click **ok** to clear the status window.

2) Click **ok** to return to **System configuration**.

b If an upgrade is available, click **yes** to upgrade your system.

CAUTION

Installation of an upgrade can take several hours to download all the software. You can continue to use Sentriant AG during the download process. Sentriant AG will automatically shutdown and restart after the software downloads.

3 After the upgrade is complete, log back in to the Sentriant AG user interface navigate to the **Test updates** window (**System configuration**>> **Test updates**).

4 Click **Check for test update**s. This ensures that your tests are current.

5 Click **ok**.

Downloading the Upgrade ISO Image

After you download the ISO image, you must burn a CD (see "Creating the Installation CD from the Sentriant AG Download" on page 2), and then perform the installation from the CD (see "Installing Sentriant AG" on page 3).

To download the upgrade ISO:

The upgrade ISO and the new ISO are the same file. See "Downloading the New Install ISO Image" on page 1.

Creating an upgrade CD from the download

To burn the upgrade ISO image to a CD:

Follow the process described in "Creating the Installation CD from the Sentriant AG Download" on page 2.

Upgrading from a CD

To upgrade from a system running 4.x, perform the following steps:

Command line window

1 Place the install CD in the filesystem that is NOT the generic `mnt` area. See http://www.linux.com/base/ldp/howto/CDROM-HOWTO/x289.html#AEN980 for more information on Linux `mnt`.

2 Log in to the Sentriant AG MS as `root` using SSH or directly using a keyboard.

3 Enter the following commands at the command line:

```
mkdir /mntl/cdrom
mount /dev/cdrom /mntl/cdrom
```

4 Follow the instructions in the *Sentriant AG Installation Guide Upgrading from the Command Line*.

5 If the server needs to reboot it will ask you to do that.

To upgrade from a system running 5.0-40103 to (but not including) 5.0-40110, perform the following steps:

Command line window

1 Place the install CD in the filesystem that is NOT the generic `mnt` area. See http://www.linux.com/base/ldp/howto/CDROM-HOWTO/x289.html#AEN980 for more information on Linux `mnt`.

2 Log in to the Sentriant AG MS as `root` using SSH or directly using a keyboard.

3 Enter the following command at the command line:

```
setProperty.py -m Compliance.UpgradeManager.CDRomMountPoint=/mntl
```

4 From a different computer with browser software installed, log in to the Sentriant AG user interface.

5 Follow the instructions in the *Sentriant AG Installation Guide Upgrading from the Sentriant AG User Interface*.

6 Enter the following command at the command line:

```
set Property.py -m Compliance.UpgradeManager.CDRomMountPoint=/mnt/cdrom
```

To upgrade from a system running 5.0-40110 or later perform the following steps:

Command line window

1 Place the install CD in the filesystem where the generic `mnt` area is defined. See http://www.linux.com/base/ldp/howto/CDROM-HOWTO/x289.html#AEN980 for more information on Linux `mnt`.

2 Log in to the Sentriant AG MS as `root` using SSH or directly using a keyboard.

3 Enter the following commands at the command line:

```
mkdir /mnt/cdrom
mount /dev/cdrom /mnt/cdrom
```

4 From a different computer with browser software installed, log in to the Sentriant AG user interface.

5 Follow the instructions in the *Sentriant AG Installation Guide Upgrading from the Sentriant AG User Interface*.

If you have questions or experience problems, contact Extreme Networks, Inc. Technical Assistance Center (TAC) at support@extremenetworks.com or call (800) 998-2408.

1 Configuring Sentriant AG

The System configuration window allows you to set the Sentriant AG operating parameters

Sentriant AG Home window>>System configuration

The *Sentriant AG Users Guide* provides detailed instructions for configuring Sentriant AG.

If you experience problems, or have questions, contact Extreme Networks, Inc. Technical Assistance Center (TAC) (support@extremenetworks.com or call (800) 998-2408).

1 Installation and Configuration Check List

Minimum System Requirements

Required fields are indicated by a red asterisk (*).

□ Dedicated server *
with:

- □ Processor (Intel Dual Core (Core 2 Duo/Xeon 5100 series)) *: ______________________________
- □ Speed (1.86) *: ____
- □ Memory (21 GB RAM) *: ____
- □ Disk space (8036 GBSATA disk drive (or greater)) *:______________________________
- □ Two (standard/802.1X) server-quality NIC cards (Intel) *: _______________________
- □ CD-ROM drive *

□ Internet connection with outbound SSL communications *
NOTE: You must have access to the following:

- □ For license validation and test updates:
  http://update.sentriantag.extremenetworks.com port 443 *
- □ For software and operating system updates:
  http://download.sentriantag.extremenetworks.com port 80 *

□ Workstation running one of the following browsers with 128-bit encryption: *

- □ Windows:
  Mozilla Firefox 1.5 or later
  Mozilla 1.7
  Internet Explorer 6.0
- □ Linux:
  Mozilla Firefox 1.5 or later
  Mozilla 1.7
- □ Mac OS X:
  Mozilla Firefox 1.5 or later

□ License key: * (cut and paste from the email you receive from Extreme Networks, Inc.)

Installation Location

□ My office(s)
□ Server room(s)/Data center(s)
□ Test lab(s)
□ Production network(s)

□ I have access to the installation site(s)
□ I do not have access to the installation site(s)

Installation Media

Required fields are indicated by a red asterisk (*).

□ One of the following: *
  □ Install CD
  □ Upgrade link: (provided to Extreme Networks, Inc. subscribers through email)

IP Addresses, Hostname, Logins, and Passwords

NOTE

This Installation and Configuration Checklist is a list of the items used in Sentriant AG including passwords; however, Extreme Networks, Inc. recommends as a security best practice that you never write down passwords.

Single-server Installation

Required fields are indicated by a red asterisk (*).

The MS and ES are installed on the same physical server.

□ MS/ES IP address: * ______________________________
□ MS/ES Netmask IP address (Network mask): * ______________________________
□ Cluster name: * ______________________________
□ Default gateway IP address: * ______________________________
□ Primary nameserver IP address (DNS server): * ______________________________
□ Secondary nameserver IP address (DNS server): ______________________________
□ Tertiary nameserver IP address (DNS server): ______________________________
□ MS/ES hostname (FQDN): * ______________________________

NOTE

Select simple names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

□ Time zone: * ______________________________
□ MS/ES server root password: * ______________________________
□ MS/ES Database password:* ______________________________

❒ Sentriant AG user interface administrator account name: * ______________________________

❒ Sentriant AG user interface administrator account password: * __________________________

❒ SMTP server IP address: ____

Multiple-server Installations

Required fields are indicated by a red asterisk (*).

The MS is installed on one physical server; each ES is installed on a unique physical server.

Management Server

Required fields are indicated by a red asterisk (*).

Create at least one MS.

❒ MS IP address: * ____

❒ MS Netmask IP address (Network mask): * ____

❒ Default gateway IP address: * ____

❒ Primary nameserver IP address (DNS server): * ______________________________________

❒ Secondary nameserver IP address (DNS server): _______________________________________

❒ Tertiary nameserver IP address (DNS server): ____

❒ MS hostname (FQDN): * ____

NOTE

Select simple names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

❒ Time zone: * ____

❒ MS server root password: * ____

❒ MS Database password:* ____

❒ Sentriant AG user interface administrator account name: * ______________________________

❒ Sentriant AG user interface administrator account password: * __________________________

❒ SMTP server IP address: ____

Enforcement Server 1

Required fields are indicated by a red asterisk (*).

Create at least one ES.

❒ Cluster name 1: * ____

❒ ES IP address: * ____

□ ES Netmask IP address (Network mask): * ____________________

□ Default gateway IP address: * ____________________

□ Primary nameserver IP address (DNS server): * ____________________

□ Secondary nameserver IP address (DNS server): ____________________

□ Tertiary nameserver IP address (DNS server): ____________________

□ ES hostname (FQDN): * ____________________

NOTE

Select simple names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

□ Time zone: * ____________________

□ ES server root password: * ____________________

□ ES Database password:* ____________________

□ Sentriant AG user interface administrator account name: * ____________________

□ Sentriant AG user interface administrator account password: * ____________________

Enforcement Server 2

Required fields are indicated by a red asterisk (*).

Create at least one ES.

□ Cluster name 2: * ____________________

□ ES IP address: * ____________________

□ ES Netmask IP address (Network mask): * ____________________

□ Default gateway IP address: * ____________________

□ Primary nameserver IP address (DNS server): * ____________________

□ Secondary nameserver IP address (DNS server): ____________________

□ Tertiary nameserver IP address (DNS server): ____________________

□ ES hostname (FQDN): * ____________________

□ Time zone: * ____________________

□ ES server root password: * ____________________

□ ES Database password:* ____________________

□ Sentriant AG user interface administrator account name: * ____________________

□ Sentriant AG user interface administrator account password: * ____________________

Enforcement Server 3

Required fields are indicated by a red asterisk (*).

Create at least one ES.

- □ Cluster name 3: * ______________________________
- □ ES IP address: * ______________________________
- □ ES Netmask IP address (Network mask): * ______________________________
- □ Default gateway IP address: * ______________________________
- □ Primary nameserver IP address (DNS server): * ______________________________
- □ Secondary nameserver IP address (DNS server): ______________________________
- □ Tertiary nameserver IP address (DNS server): ______________________________
- □ ES hostname (FQDN): * ______________________________
- □ Time zone: * ______________________________
- □ ES server root password: * ______________________________
- □ ES Database password: * ______________________________
- □ Sentriant AG user interface administrator account name: * ______________________________
- □ Sentriant AG user interface administrator account password: * ______________________________

Proxy Server

Required fields are indicated by a red asterisk (*).

If you use a proxy server for Internet connections, these fields are required:

- □ Proxy server IP address: * ______________________________
- □ Proxy server port: * ______________________________
- □ Proxy server authentication method (basic or digest): * ______________________________
- □ Proxy server user ID: * ______________________________
- □ Proxy server password: * ______________________________

Agentless Credentials

Required fields are indicated by a red asterisk (*).

The administrator credentials for endpoints on a domain. Set them globally for all clusters, or override them on a per-cluster basis.

- □ All clusters:
  - □ Windows domain name: * ______________________________
  - □ Administrator user ID: * ______________________________
  - □ Administrator password: * ______________________________
- □ Cluster 1:
  - □ Windows domain name: * ______________________________

- ❐ Administrator user ID: * ____
- ❐ Administrator password: * ____

❐ Cluster 2:

- ❐ Windows domain name: * ____
- ❐ Administrator user ID: * ____
- ❐ Administrator password: * ____

❐ Cluster 3:

- ❐ Windows domain name: * ____
- ❐ Administrator user ID: * ____
- ❐ Administrator password: * ____

❐ Cluster 4:

- ❐ Windows domain name: * ____
- ❐ Administrator user ID: * ____
- ❐ Administrator password: * ____

Quarantine

Define quarantine methods and settings for all clusters, or on a per-cluster basis.

802.1X

Required fields are indicated by a red asterisk (*).

❐ Quarantine subnets: ____

❐ RADIUS server type (local or remote IAS): ____

❐ Local RADIUS server type end-user authentication method:

- ❐ Manual: ____
- ❐ Windows domain:
  - ❐ Domain name: * ____
  - ❐ Administrator user name: * ____
  - ❐ Administrator password: * ____
  - ❐ Domain controllers: * ____
  - ❐ Additional credentials user name: * ____
  - ❐ Additional credentials password: * ____
- ❐ Open LDAP:
  - ❐ Server: * ____
  - ❐ Identity: * ____
  - ❐ Password: * ____
  - ❐ Base DN: * ____

- ❒ Filter: * ____
- ❒ Password attribute: * ____
- ❒ End-user credentials user name: * __________________________________
- ❒ End-user credentials Password: * __________________________________

802.1X Devices

Required fields are indicated by a red asterisk (*).

Define 802.1X devices globally for all clusters, or on a per-cluster basis.

- ❒ 802.1X device 1
  - ❒ IP address: * ____
  - ❒ Shared secret: * ____
  - ❒ Device type: * ____
- ❒ 802.1X device 2
  - ❒ IP address: * ____
  - ❒ Shared secret: * ____
  - ❒ Device type: * ____
- ❒ 802.1X device 3
  - ❒ IP address: * ____
  - ❒ Shared secret: * ____
  - ❒ Device type: * ____
- ❒ 802.1X device 4
  - ❒ IP address: * ____
  - ❒ Shared secret: * ____
  - ❒ Device type: * ____
- ❒ 802.1X device 5
  - ❒ IP address: * ____
  - ❒ Shared secret: * ____
  - ❒ Device type: * ____

DHCP

Required fields are indicated by a red asterisk (*).

Define quarantine areas for all clusters, or on a per-cluster basis. Create as many quarantine areas as you need.

NOTE

If you select DHCP quarantine, you must create at least one area or you will get a process error.

- ❒ DHCP quarantine area 1:*
  - ❒ Quarantine area 1 quarantined subnet: * ________________________________
  - ❒ Quarantine area 1 DHCP IP range: * ____________________________________
  - ❒ Quarantine area 1 quarantined area gateway: * ___________________________
  - ❒ Quarantine area 1 domain suffix: * ____________________________________
  - ❒ Quarantine area 1 corresponding non-quarantined subnets: * _____________
- ❒ DHCP quarantine area 2:
  - ❒ Quarantine area 2 quarantined subnet: __________________________________
  - ❒ Quarantine area 2 DHCP IP range: * ____________________________________
  - ❒ Quarantine area 2 quarantined area gateway: ____________________________
  - ❒ Quarantine area 2 domain suffix: * ____________________________________
  - ❒ Quarantine area 2 corresponding non-quarantined subnets:_______________
- ❒ DHCP quarantine area 3:
  - ❒ Quarantine area 3 quarantined subnet: __________________________________
  - ❒ Quarantine area 3 DHCP IP range: * ____________________________________
  - ❒ Quarantine area 3 quarantined area gateway: ____________________________
  - ❒ Quarantine area 3 domain suffix: * ____________________________________
  - ❒ Quarantine area 3 corresponding non-quarantined subnets:_______________

Accessible services

Accessible services are defined for all clusters or on a per-cluster basis.

- ❒ Accessible services and endpoints for all clusters:
  - ❒ Web sites:____
  - ❒ Hostnames: ____
  - ❒ IP addresses / ports: ____
  - ❒ Networks: ____
  - ❒ Windows domain controller: ____
- ❒ Accessible services and endpoints for cluster 1:
  - ❒ Web sites:____
  - ❒ Hostnames: ____
  - ❒ IP addresses / ports: ____
  - ❒ Networks: ____

- ❒ Windows domain controller: ______________________________

❒ Accessible services and endpoints for cluster 2:

- ❒ Web sites: ______________________________
- ❒ Hostnames: ______________________________
- ❒ IP addresses / ports: ______________________________
- ❒ Networks: ______________________________
- ❒ Windows domain controller: ______________________________

❒ Accessible services and endpoints for cluster 3:

- ❒ Web sites: ______________________________
- ❒ Hostnames: ______________________________
- ❒ IP addresses / ports: ______________________________
- ❒ Networks: ______________________________
- ❒ Windows domain controller: ______________________________

Notifications

Notifications are defined for all clusters or on a per-cluster basis.

❒ All clusters

- ❒ Send information to: ______________________________
- ❒ SNMP server IP address: ______________________________
- ❒ Email information sent from: ______________________________

❒ Cluster 1

- ❒ Send information to: ______________________________
- ❒ SNMP server IP address: ______________________________
- ❒ Email information sent from: ______________________________

❒ Cluster 2

- ❒ Send information to: ______________________________
- ❒ SNMP server IP address: ______________________________
- ❒ Email information sent from: ______________________________

❒ Cluster 3

- ❒ Send information to: ______________________________
- ❒ SNMP server IP address: ______________________________
- ❒ Email information sent from: ______________________________

Test Exceptions

Exceptions are defined for all clusters or on a per-cluster basis.

- ❐ All cluster endpoint testing exceptions (endpoints that are whitelisted or blacklisted):
  - ❐ MAC addresses: ______________________________
  - ❐ IP addresses: ______________________________
  - ❐ NetBIOS names: ______________________________
- ❐ Cluster 1 endpoint testing exceptions (endpoints that are whitelisted or blacklisted):
  - ❐ MAC addresses: ______________________________
  - ❐ IP addresses: ______________________________
  - ❐ NetBIOS names: ______________________________
- ❐ Cluster 2 endpoint testing exceptions (endpoints that are whitelisted or blacklisted):
  - ❐ MAC addresses: ______________________________
  - ❐ IP addresses: ______________________________
  - ❐ NetBIOS names: ______________________________
- ❐ Cluster 3 endpoint testing exceptions (endpoints that are whitelisted or blacklisted):
  - ❐ MAC addresses: ______________________________
  - ❐ IP addresses: ______________________________
  - ❐ NetBIOS names: ______________________________

Index

Numerics

802.1x 1, 8
  deployment 1

A

Active Content 6
active content
  change IE security settings 6
add
  ES to cluster 22
allow pop-up windows 5
allowing
  pop-up windows in Windows or Linux 5
authentication 4

B

browser
  allow pop-ups 4
browser settings 4
built-in RADIUS server 8

C

CD
  create 2
CD, install 1
change
  IE security settings for active content 6
configure
  MS/ES 14
create
  CD of upgrade ISO 29
  Enforcement cluster 19
  install CD 2
  installation CD for upgrade but no Internet connection v4.x 26
  installation CD for upgrade but no Internet connection v5.0 26
creating
  installation CD 2

D

DAC 4, 9
Device Activity Capture 9
DHCP 4, 8
  deployment 1
download 26
  ISO 1
  upgrade ISO 29
downloading the upgrade ISO image 29

E

ES
  add to cluster 22
ethtool
  determining eth0 and eth1 13

F

Figure
  802.1X Enforcement 10
  Accept License Agreement Window 16
  Add Enforcement Cluster Window 22
  Add Enforcement Server Window 23
  Create Administrator Account Window 19
  Enforcement Clusters & Servers 21
  Enter License Key Window 18
  Enter Management Server Settings Window 17
  Home Window 20
  IE Internet Options, Advanced Tab 6
  IE Security Message Options 6
  IE Security Warning Pop-up Window 6
  Install Screen, Boot Prompt 7
  Install Screen, Hostname Configuration 10
  Install Screen, Installation Confirmation 8
  Install Screen, Installation Progress 13
  Install Screen, Installation Type 12
  Install Screen, Miscellaneous Network Settings 9
  Install Screen, Network Configuration for eth0 9
  Install Screen, Root Password 12
  Install Screen, Time Zone Select 11
  Internet Explorer Security Warning Message 5
  Multiple-server Installation, Quarantine Method, DHCP 3
  Multiple-server Installation, Quarantine Method, Inline 2

Security Alert Window 15
Single-server Installation, DHCP Mode, Complex Example 7
Single-server Installation, DHCP Mode, Simple Example 6
Single-server Installation, Endpoint Static Route Enforcement 8
Single-server Installation, Ethernet Card Installation, 802.1X 13
Single-server Installation, Ethernet Card Installation, DHCP 12
Single-server Installation, Ethernet Card Installation, Inline 11
Single-server Installation, Quarantine Method, DHCP, Flat Network 3
Single-server Installation, Quarantine Method, Inline 2
System Configuration Window, Management Server Option 28
System Configuration, Enforcement Clusters & Servers Window 24
Firefox, supported version 1
firewall
onboard 4
FQDN 2, 3, 4, 5

G

Gateway
deployment 1
gateway 4

H

hardened operating system 1
hardware
required 1

I

IAS plug-in 8
IE
minimum font size 7
IE security settings
allow for active content 6
Inline
deployment 1
inline 1
install 3
CD 1
upgrade from command line 26
install CD 1
installation
CD, creating from the ISO download 2
first time 1
upgrade 1
IP address
static 8
IP addresses 1

L

license
key 3
license validation and test updates 1

M

minimum requirements 1
Mozilla
minimum font size 7
Mozilla, supported version 1
multiple-server environment 13

N

name
Enforcement cluster 19
NIC 11
recommended types 13

O

operating system, hardened 1

P

page caching 8
Mozilla options 8
ping 14
pop-up window 4
pop-up windows
allow in Mac Firefox 5
pop-up windows, allowing 4
proxy to any other RADIUS 8

R

RAS 4
reboot 6
required
hardware 1
software 1

S

single-server environment 6
software and operating system updates 1
SSL 15
static IP addresses 8
static route
    add to server 15
static routes 4
system
    requirements 1

T

temporary files 8
    delete in Mac Firefox 9
    delete in Mozilla 9
    delete in Windows or Linux Firefox 9

U

upgrade
    from user interface 27
    with Internet connection 25
upgrade ISO
    burn to CD 29
    download 29
upgrade without an Internet connection 25
upgrading from the command line 27
Users' guide 1

V

verify
    server requirements 4
VPN 4